

(19)日本国特許庁 (J P)

(12)公表特許公報 (A)

(11)特許出願公表番号  
特表2003-536144  
(P2003-536144A)

(43)公表日 平成15年12月2日(2003.12.2)

| (51)Int.Cl. <sup>7</sup>           | 識別記号  | F I           | テーマコード <sup>*</sup> (参考) |           |
|------------------------------------|-------|---------------|--------------------------|-----------|
| G 0 6 F 12/14                      | 3 2 0 | G 0 6 F 12/14 | 3 2 0 F                  | 5 B 0 1 7 |
|                                    |       |               | 3 2 0 B                  | 5 B 0 3 5 |
| 17/60                              | 1 4 2 | 17/60         | 1 4 2                    | 5 B 0 5 8 |
|                                    | 5 1 0 |               | 5 1 0                    |           |
|                                    | 5 1 2 |               | 5 1 2                    |           |
| 審査請求 未請求 予備審査請求 未請求(全 68 頁) 最終頁に続く |       |               |                          |           |

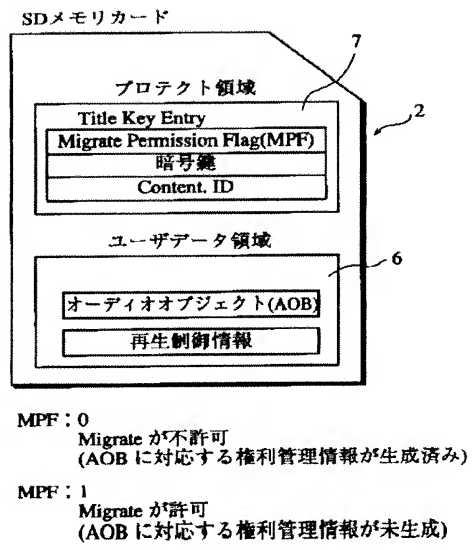
|             |  |         |                        |
|-------------|--|---------|------------------------|
| (21)出願番号    | 特願2002-502671(P2002-502671)  | (71)出願人 | 松下電器産業株式会社             |
| (86)(22)出願日 | 平成13年5月30日(2001.5.30)  |         | 大阪府門真市大字門真1006番地       |
| (85)翻訳文提出日  | 平成14年1月29日(2002.1.29)  | (72)発明者 | 松島 秀樹                  |
| (86)国際出願番号  | P C T / U S 0 1 / 1 7 2 9 1  |         | 大阪府枚方市東香里3-11-30       |
| (87)国際公開番号  | W O 0 1 / 0 9 5 2 0 6  | (72)発明者 | 原田 俊治                  |
| (87)国際公開日   | 平成13年12月13日(2001.12.13)  |         | 大阪府大阪市西成区玉出西2-20-52    |
| (31)優先権主張番号 | 0 9 / 5 8 5 , 4 2 4  | (72)発明者 | 上坂 靖                   |
| (32)優先日     | 平成12年6月2日(2000.6.2)  |         | 兵庫県三田市つつじが丘北2丁目16番地16号 |
| (33)優先権主張国  | 米国 (U S)   | (72)発明者 | 廣田 照人                  |
| (81)指定国     | E P (A T , B E , C H , C Y , D E , D K , E S , F I , F R , G B , G R , I E , I T , L U , M C , N L , P T , S E , T R ) , A U , C N , I D , J P , K R , M X , U S , V N |         | 大阪府守口市梶町1-20-1-306     |
|             |  | (74)代理人 | 弁理士 中島 司朗              |
|             |  | 最終頁に続く  |                        |

(54)【発明の名称】 記録媒体、ライセンス管理装置、記録再生装置

(57)【要約】

【課題】1つのオーディオオブジェクトの権利管理情報がLCMにより二重、三重に管理されることを避けつつ、Migrateの実行をPDにより生成されたオーディオオブジェクトに限定することができるような情報体系を有する記録媒体を提供する。

【解決手段】ライセンス管理装置を含むSDMIシステムにおいて用いられる記録媒体(半導体メモリカード)であり、対応するRMIがライセンス管理装置により既に生成されているAOBと、対応するRMIが存在しないAOBとが記録されている。各AOBにはMPFが対応づけており、対応するAOBが後者である場合、オンに設定されてMigrate処理が許可されている旨を示し、対応するAOBが前者である場合、オフに設定されてMigrate処理が許可されていない旨を示す。



**【特許請求の範囲】**

【請求項1】 複数の装置と共に用いられる記録媒体であり、  
オーディオオブジェクトと、

オーディオオブジェクトについての権利管理情報が、前記複数装置の何れかにより既に生成されている場合、オフに設定されてマイグレイト処理が許可されていない旨を示し、オーディオオブジェクトについての権利管理情報が未生成である場合、オンに設定されてマイグレイト処理が許可されている旨を示すフラグとが記録されている記録媒体。

【請求項2】 前記記録媒体は半導体メモリカードであり、  
何れかの装置が接続された際、その装置が正当か否かを認証する認証回路と、正当であることが認証回路により認証された場合のみ、アクセスされるプロテクト領域とを備え、

前記フラグは、プロテクト領域に記録されている請求項1記載の記録媒体。

【請求項3】 プロテクト領域には、フラグと共に暗号鍵が記録されており、  
前記オーディオオブジェクトは、プロテクト領域に記録されている暗号鍵を用いて暗号化された暗号化オーディオデータである請求項2記載の記録媒体。

【請求項4】 ライセンス管理装置であって、  
オーディオオブジェクトと、オーディオオブジェクトに対応するフラグとが記録された記録媒体を接続する接続手段と、

フラグの設定値を参照することにより、記録媒体に記録されているオーディオオブジェクトについてのマイグレイト処理が許可されているか、許可されていないかを判定する第1判定手段と、

格納手段と、

マイグレイト処理が許可されている場合のみ、記録媒体からオーディオオブジェクトを読み出すとともに、そのオーディオオブジェクトについての権利管理情報を生成して、当該読み出されたオーディオオブジェクトと、権利管理情報とを対応付けて格納手段に書き込むことによりマイグレイト処理を実行するマイグレイト処理手段と

を含むライセンス管理装置。

【請求項5】 前記ライセンス管理装置は、  
マイグレイト処理が許可されていない場合、オーディオオブジェクトについての権利管理情報を自機が既に生成しているか否かを判定する第2判定手段と、  
自機により生成されている場合、権利管理情報に含まれるチェックアウト許可回数をインクリメントして、記録媒体におけるオーディオオブジェクトを再生不能な状態にすることによりチェックインを行うチェックイン手段と  
を含む請求項4記載のライセンス管理装置。

【請求項6】 ライセンス管理装置と共に用いられ、対応する権利管理情報がライセンス管理装置により既に生成されている第1のオーディオオブジェクトと、オフに設定されたフラグとが記録された記録媒体に対して読み書きを行う記録再生装置であって、

ユーザにより再生指示がなされた場合、記録媒体に記録されている第1のオーディオオブジェクトを再生する再生手段と、

ユーザにより記録指示がなされた場合、音声信号を装置外部から受け付ける信号受付手段と、

音声信号を符号化することにより、第2のオーディオオブジェクトを得る符号化手段と、

オーディオオブジェクトの取り込みと、権利管理情報の生成とを行う処理であるマイグレイト処理が許可されている旨を示すフラグを対応づけて、第2のオーディオオブジェクトを記録媒体に記録する書込手段と

を含む記録再生装置。

【請求項7】 前記記録再生装置は、他の記録媒体に記録されたパッケージコンテンツを再生する再生装置と共に用いられ、

信号受付手段は、

再生装置に対して再生指示がなされ、自装置に対して記録指示がなされた場合に、パッケージコンテンツが再生されることにより得られる音声信号を再生装置から受け付け、

前記符号化手段は、

音声信号を符号化してゆくことにより、第2のオーディオオブジェクトを得る

請求項6記載の記録再生装置。

【請求項8】 オーディオオブジェクトと、オーディオオブジェクトに対応するフラグとが記録された記録媒体を接続する接続手段、格納手段を有するコンピュータに

フラグの設定値を参照することにより、記録媒体に記録されているオーディオオブジェクトについてのマイグレイト処理が許可されているか、許可されていないかを判定する第1判定ステップと、

マイグレイト処理が許可されている場合のみ、記録媒体からオーディオオブジェクトを読み出すとともに、そのオーディオオブジェクトについての権利管理情報を生成して、当該読み出されたオーディオオブジェクトと、権利管理情報とを対応付けて格納手段に書き込むマイグレイト処理を行うマイグレイト処理ステップと

を行わせるライセンス管理プログラムを記録したコンピュータ読取可能な記録媒体。

【請求項9】 前記ライセンス管理プログラムは、

マイグレイト処理が許可されていない場合、オーディオオブジェクトについての権利管理情報を自機が既に生成しているか否かを判定する第2判定ステップと、

自機により生成されている場合、権利管理情報に含まれるチェックアウト許可回数をインクリメントして、記録媒体におけるオーディオオブジェクトを再生不能な状態にすることによりチェックインを行うチェックインステップと

を行わせる請求項8記載のコンピュータ読取可能な記録媒体。

【請求項10】 オーディオオブジェクトと、オーディオオブジェクトに対応するフラグとが記録された記録媒体を接続する接続手段、格納手段を有するコンピュータにライセンス管理を行わせる管理方法であって、

フラグの設定値を参照することにより、記録媒体に記録されているオーディオオブジェクトについてのマイグレイト処理が許可されているか、許可されていないかを判定する第1判定ステップと、

マイグレイト処理が許可されている場合のみ、記録媒体からオーディオオブジ



ェクトを読み出すとともに、そのオーディオオブジェクトについての権利管理情報を生成して、当該読み出されたオーディオオブジェクトと、権利管理情報とを対応付けて格納手段に書き込むことによりマイグレイト処理を行うマイグレイト処理ステップと

を含む管理方法。

【請求項11】 前記管理方法は、

マイグレイト処理が許可されていない場合、オーディオオブジェクトについての権利管理情報を自機が既に生成しているか否かを判定する第2判定ステップと

、  
自機により生成されている場合、権利管理情報に含まれるチェックアウト許可回数をインクリメントして、記録媒体におけるオーディオオブジェクトを再生不能な状態にすることによりチェックインを行うチェックインステップと

を含む請求項10記載の管理方法。

【請求項12】 複数の装置と共に用いられる記録媒体であって

ストリームデータと、

ストリームデータについての権利管理情報が、前記複数装置の何れかにより既に生成されている場合、オフに設定されてマイグレイト処理が許可されていない旨を示し、ストリームデータについての権利管理情報が未生成である場合、オンに設定されてマイグレイト処理が許可されている旨を示すフラグとが

記録されている記録媒体。

【請求項13】 ライセンス管理装置であって、

ストリームデータと、ストリームデータに対応するフラグとが記録された記録媒体を接続する接続手段と、

フラグの設定値を参照することにより、記録媒体に記録されているストリームデータについてのマイグレイト処理が許可されているか、許可されていないかを判定する第1判定手段と、

格納手段と、

マイグレイト処理が許可されている場合のみ、記録媒体からストリームデータを読み出すとともに、そのストリームデータについての権利管理情報を生成して、

当該読み出されたストリームデータと、権利管理情報とを対応付けて格納手段に書き込むことによりマイグレイト処理を実行するマイグレイト処理手段とを含むライセンス管理装置。

【請求項14】 ライセンス管理装置と共ににおいて用いられ、対応する権利管理情報がライセンス管理装置により既に生成されている第1のストリームデータと、オフに設定されたフラグとが記録された記録媒体に対して読み書きを行う記録再生装置であって、

ユーザにより再生指示がなされた場合、記録媒体に記録されている第1のストリームデータを再生する再生手段と、

ユーザにより記録指示がなされた場合、音声信号の入力を装置外部から受け付ける信号入力受付手段と、

入力される音声信号を符号化することにより、第2のストリームデータを得る符号化手段と、

ライセンス管理装置内部へのストリームデータの取り込みと、ライセンス管理装置が権利管理情報の生成とを行う処理であるマイグレイト処理が許可された旨を示すフラグを対応づけて、第2のストリームデータを記録媒体に記録する書込手段と

を含む記録再生装置。

**【発明の詳細な説明】****(技術分野)**

本発明は、記録媒体、ライセンス管理装置、記録再生装置に関し、CDやDVD-Audioに記録されたパッケージコンテンツのバックアップとして得られたオーディオデータを記録する場合の改良に関する。

**【0001】****(背景技術)**

MP3等の圧縮コーデックを用いたCDのバックアップ技術は、皮肉なことながら、コンテンツの著作権者の利益を脅かす存在になりつつある。これは、バックアップのために得られたオーディオデータが著作権者に無断でインターネット等を通じて流通されるという行為が、世界中で散見されるからである。こうした現状を踏まえ、SDMI (Secure Digital Music Initiative) では、CDに記録されたパッケージコンテンツのバックアップを、以下の2通りの方法で行うよう規定している。

**【0002】**

1つ目の方法とは、ライセンス管理装置がCDのバックアップをとるというもの、2つ目の方法とは、ポータブルデバイスがCDのバックアップをとるというものである。ライセンス管理装置とは、Licensed Compliantモジュール (以下LCMという) と呼ばれるソフトウェアを具備したパソコン等の機器であり、ポータブルデバイス (Portable Device (以下PDという)) とはLCMを具備していない音響機器である。LCMを有しているため、ライセンス管理装置は、バックアップにより得られたオーディオデータを管理する機能を有している。具体的にいうなら、バックアップ用オーディオデータについての権利管理情報を生成し、これを更新するという機能を有する。一方PDはLCMを有さないため、PDはかかる管理機能を有さず、オーディオデータの記録・再生といった処理のみに機能が限定されている。これらPD、ライセンス管理装置は何れも、パッケージコンテンツを圧縮符号化することにより得られたオーディオデータを所定の暗号鍵を用いて暗号化した上で記録媒体に記録する。PD、ライセンス管理装置は、この記録媒体から別の記録媒体へのオーディオデータのコピーを原則として禁ずる。故にバックアップ用のオーデ

ィオデータがインターネット上で流通することは有り得ない。このコピー禁止の原則に対する例外は、ライセンス管理装置によって行われるチェックアウト・チェックイン処理である。チェックアウトとは、恰も宿泊客がホテルから外出するかの如く、ライセンス管理装置内部で管理されているバックアップのためのオーディオデータを、半導体メモリカード等の可搬型記録媒体に記録する行為であり、これにより、バックアップ用のオーディオデータをライセンス管理装置の外に出すことができ、PDでも利用できることになる。逆にチェックインとは、宿泊客を外出先からホテルに呼び戻すかの如く、可搬型記録媒体に記録されたバックアップオーディオデータを、ライセンス管理装置内部に取り込む行為である。可搬型記録媒体に記録されたオーディオデータをライセンス管理装置内部に取り込ませることにより、可搬型記録媒体に、他のオーディオデータを記録して利用することができる。

#### 【0003】

ところでPDは、権利管理を行えないので、PDにてバックアップを行った場合は、チェックアウト・チェックインのような例外的なコピーが一切を行えず、ライセンス管理装置を用いてバックアップをとる技術と比較して、使い勝手が悪いという心証をユーザに与えているという問題点があった。

#### (発明の開示)

上述した問題点を解決するため、PDが記録したオーディオデータに対してライセンス管理装置がMigrateを行うことも考えられる。Migrateとは、ライセンス管理装置が記録媒体に記録されているオーディオデータについての権利管理情報の生成を行い、オーディオデータを、その権利管理情報に対応づけて、そのライセンス管理装置の管理下に置くことである。しかし、PDにより記録されたオーディオデータと、ライセンス管理装置のチェックアウトにより記録されたオーディオデータとが同一の記録媒体に記録されており、これに対してライセンス管理装置がMigrateを行おうとする場合、以下のような問題が生じる。つまりPDにより記録されたオーディオオブジェクトに対してMigrateが行われることに問題はないが、同じ記録媒体にチェックアウトにより得られたオーディオオブジェクトが記録されていたとすると、このチェックアウトにより得られたオーディオオブジェ

クトに対してもMigrateが行われる恐れがある。

【0004】

チェックアウトにより得られたオーディオオブジェクトは、既に何れかのライセンス管理装置に権利管理情報が格納されているので、これに対してMigrateが行われれば、1つのオーディオオブジェクトに対して権利管理情報が二重に生成されることになる。権利管理情報には、例えば3回というオーダーのチェックアウト許可回数が含まれているので、既に権利管理情報が生成されているオーディオオブジェクトに対してMigrateが2回、3回と行われ、二重、三重に権利管理情報が生成されれば、実質6回、9回のチェックアウトが許可されることになる。これでは、チェックアウトが必要以上に行われるばかりか、コピーの無限連鎖を招きかねない。

【0005】

本発明の目的は、1つのオーディオオブジェクトの権利管理情報がLCMにより二重、三重に管理されることを避けつつ、Migrateの実行をPDにより生成されたオーディオオブジェクトに限定することができるような情報体系を有する記録媒体を提供することである。

上記目的は、オーディオオブジェクトと、オーディオオブジェクトについての権利管理情報が、前記複数装置の何れかにより既に生成されている場合、オフに設定されてマイグレート処理が許可されていない旨を示し、オーディオオブジェクトについての権利管理情報が未生成である場合、オンに設定されてマイグレート処理が許可されている旨を示すフラグとが記録されている記録媒体により達成される。この記録媒体によれば、フラグに、各オーディオオブジェクトについてMigrateの要否が示されているので、これに従えば、Migrateは権利管理情報が存在しないオーディオオブジェクトに対して、一回限り許可されることになる。よって権利管理情報が既に存在するオーディオオブジェクトに対して、重複して権利管理情報が生成されることはない。これにより、著作権保護の観念に反することなく、チェックアウトにより得られたオーディオオブジェクトと、PDにより得られたオーディオオブジェクトとを同じ記録媒体に記録することができる。

【0006】

ここでオーディオオブジェクトと、オーディオオブジェクトに対応するフラグとが記録された記録媒体を接続する接続手段と、フラグの設定値を参照することにより、記録媒体に記録されているオーディオオブジェクトについてのマイグレイト処理が許可されているか、許可されていないかを判定する第1判定手段と、格納手段と、マイグレイト処理が許可されている場合のみ、記録媒体からオーディオオブジェクトを読み出すとともに、そのオーディオオブジェクトについての権利管理情報を生成して、当該読み出されたオーディオオブジェクトと、権利管理情報とを対応付けて格納手段に書き込むことによりマイグレイト処理を実行するマイグレイト処理手段とを含むライセンス管理装置を構成してもよい。このライセンス管理装置によれば、記録再生装置が音声信号を圧縮符号化することにより得られたオーディオオブジェクトについては、圧縮符号化を重複して行うことなく、オーディオオブジェクトを得ることができる。ライセンス管理装置がオーディオオブジェクトを得るまでの期間を短縮することができるので、ユーザにとっての利便性が向上する。

#### 【0007】

ここでライセンス管理装置と共に用いられ、対応する権利管理情報がライセンス管理装置により既に生成されている第1のオーディオオブジェクトと、オフに設定されたフラグとが記録された記録媒体に対して読み書きを行う記録再生装置であって、ユーザにより再生指示がなされた場合、記録媒体に記録されている第1のオーディオオブジェクトを再生する再生手段と、ユーザにより記録指示がなされた場合、音声信号を装置外部から受け付ける信号受付手段と、音声信号を符号化することにより、第2のオーディオオブジェクトを得る符号化手段と、オーディオオブジェクトの取り込みと、権利管理情報の生成とを行う処理であるマイグレイト処理が許可されている旨を示すフラグを対応づけて、第2のオーディオオブジェクトを記録媒体に記録する書込手段とを含む記録再生装置を構成してもよい。この記録再生装置によれば、単にチェックアウトにより記録媒体に記録されたオーディオオブジェクトを再生するという用途に記録再生装置を用いるだけでなく、CD等に記録されているパッケージコンテンツのバックアップをとるという用途にも記録再生装置を用いることができるので、より商品価値の高い記録再

生装置を市場に提供することができる。

【0008】

(発明を実施するための最良の形態)

以下、図面を参照しながら、本発明に係る記録媒体、ライセンス管理装置1、記録再生装置(録再型PD)について説明する。本実施形態においてこれらは、SDMIシステムにおいて用いられる。SDMIシステムは、複数のSDMIドメインを含む。図1は、SDMIシステムにおける1つのSDMIドメインの構成を示す図である。図1に示すように、SDMIドメインは、ライセンス管理装置1、SDメモ리카ード2、録再型PD3、CD4、CDプレーヤ5を含む。

【0009】

ライセンス管理装置1は、SDMIプロテクトコンテンツと、権利管理情報(Right Management Information(以下RMIという))との組みを複数格納することができるローカルストレージと、LCMとを備え、チェックアウト、チェックインを行う装置であり、チェックアウト時においてオーディオオブジェクトをSDメモ리카ード2に記録する。チェックイン時においてオーディオオブジェクトを、ローカルストレージ21に取り込む。SDMIプロテクトコンテンツとは、LCM23でのみ再生可能な状態にある暗号化オーディオデータである。このオーディオデータの暗号化を解除するための暗号鍵は、RMI内に格納される。RMIは、公開鍵暗号化方式により暗号化され、RMIの暗号化は、LCM23のみが解除することができ、SDMIドメインにおいてLCM23を具備していない録再型PD3は、このRMIから暗号鍵を取り出すことができない。故にSDMIドメインにおいてSDMIプロテクトコンテンツは、LCM23でのみ再生可能なオーディオデータとして扱われることとなる。一方、オーディオオブジェクト(Audio Object(以下AOBという))とは、暗号鍵と共にSDメモ리카ード2に記録され、SDMIシステムに属する機器が再生することができる暗号化オーディオデータである。

【0010】

SDメモ리카ード2は、自身の識別のために固有の識別子(Media-IDと呼ばれる。)が記録されている記録媒体であり、システムにおいて正当と認められる機器(ライセンス管理装置1、PD3)のみがアクセスできるプロテクト領域と、正当機

器を初め、正当な機器以外の機器であっても、アクセスすることができるユーザデータ領域とを備える。

#### 【0011】

録再型PD3は、ローカルストレージ21、LCM23を有さず、SDメモリカード2に記録されているA0Bの再生と、SDメモリカード2へのA0Bの書き込みとを行うPDである。録再型PD3によりSDメモリカード2に記録されるA0Bは、CDプレーヤ5がCDを再生することにより得られる音声信号を圧縮符号化し、更に暗号化することにより得られたデータである。

#### 【0012】

CD4は、パッケージコンテンツが記録された記録媒体である。CD4に記録されているパッケージコンテンツには、SDMIによる著作権保護の対象になっているコンテンツであってWaterMarkが埋め込まれているもの、著作権保護の適用以前に作成されたコンテンツであって、WaterMarkが埋め込まれていないもの（一般にレガシーコンテンツと呼ばれる。）がある。

#### 【0013】

CDプレーヤ5は、CD4に記録されているパッケージコンテンツを再生し、音声信号を録再型PD3に出力する。またCDプレーヤ5から出力される音声信号には、IEC-958形式のデジタル信号（保護されていないデジタル信号）、アナログ信号の二種類がある。

以上のシステムにおいて特徴的なのは、CDプレーヤ5からの音声信号の圧縮符号化を録再型PD3が行い、これにより得られたA0Bを録再型PD3がSDメモリカード2に記録し、このSDメモリカード2を介してライセンス管理装置1がA0Bを取り込むという点である。

#### 【0014】

以上でSDMIシステムについての説明を終え、続いてSDメモリカード2の内部構成について説明する。図2は、SDメモリカード2の内部構成を示す図であり、本図に示すようにSDメモリカード2は、ユーザデータ領域6、プロテクト領域7を備える。

ユーザデータ領域6には、A0Bと、A0Bに対応する再生制御情報とが記録される



。プロテクト領域7には、各A0Bに対応するTitle Key Entryが記録される。Title Key Entry (以下TKEという)は、A0Bの暗号化に用いられた暗号鍵と、A0Bに対応するSDMIプロテクトコンテンツを識別するための識別子であるContent-IDと、Migrate Permission Flagとを含む。Migrate Permission Flag (MPF)は、オフに設定された際、このTKEに対応するA0Bが、複数のライセンス管理装置1のうち何れかのライセンス管理装置1のチェックアウトにより記録されたものであり、何れかのライセンス管理装置1へのMigrateが許可されていない旨を示す。MPFは、オンに設定された際、このTKEに対応するA0Bが、PDにより記録されたものであり、何れかのライセンス管理装置1へのMigrateが許可されている旨を示す。本実施形態では、オフは「0」であり、オンは「1」であるものとする。以上のA0Bと、これに対応するTKEと、再生制御情報との組みは、トラック'Track'と呼ばれる。

#### 【0015】

以上でSDメモリカード2についての説明を終え、続いて録再型PD3の内部構成について説明する。図3は、録再型PD3の内部構成を示す図である。図3に示すように録再型PD3は、SDメモリカード2の接続が可能なコネクタを備え、ユーザインターフェイス部8、信号入力端子9、スクリーニング部10 (Ripper11、WaterMark Detector12、信号ソースチェッカー13、Ripper14)、暗号化部15、録再制御部16、セキュアR/W部17、復号化部18、再生部19を備える。

#### 【0016】

ユーザインターフェイス部8は、ディスプレイ、キーパッド等で構成され、ユーザからのSDメモリカード2に対する録音指示、SDメモリカード2からの再生指示を受け付けて、これに応じた制御を暗号化部15、録再制御部16、セキュアR/W部17、復号化部18、再生部19に指示する。

信号入力端子9は、録再型PD外部から録再型PD内部へと音声信号を取り込む入力端子であり、アナログステレオタイプのもの、保護されていないデジタルタイプのもの、アナログモノラルタイプのものがある。アナログステレオタイプの入力端子及び保護されていないデジタルタイプの入力端子には、CDプレーヤ5が接続され、アナログモノラルタイプの入力端子には、マイクが接続される。

## 【0017】

スクリーニング部10は、信号入力端子9を介して録再型PD3内部に入力されてくる音声信号のうち、不法な音声信号を圧縮符号化すること避けつつ、CDプレーヤ5がCD4を再生することにより得られる音声信号やその他正当な音声信号については、オーディオデータに変換するものであり、Ripper11、WaterMark Detector12、信号ソースチェッカー13、Ripper14を含む。

## 【0018】

Ripper11は、信号入力端子9のうち、アナログステレオタイプの入力端子及び保護されていないデジタルタイプの入力端子を介して録再型PD3内部に順次入力されてくるアナログ信号、保護されていないデジタル信号をMP3 (MPEG1 Layer3)、MPEG-AAC (Advanced Audio Coding) 方式、WMA (Windows (登録商標) Media Audio) 方式等に基づき圧縮符号化して、オーディオデータを得る。

## 【0019】

WaterMark Detector12は、Ripper11から出力されたオーディオデータから、WaterMarkを検出する。Ripper11により出力されるオーディオデータが、著作権保護の対象になっているパッケージコンテンツを圧縮符号化することにより得られたものであり、WaterMark Detector12がWaterMarkを検出し得た場合、WaterMark Detector12はWaterMarkをオーディオデータから取り除き、その後オーディオデータを暗号化部15に出力する。著作権保護の対象であるパッケージコンテンツを圧縮符号化することにより得られたオーディオデータであって、WaterMarkが存在しないオーディオデータについては、Ripper11が出力したオーディオデータを暗号化部15に出力しない。何故なら、著作権保護の対象となるオーディオデータであるのに、WaterMarkが存在しないということは、このオーディオデータは過去にスクリーニング部10を通過しており、既にWaterMarkが取り除かれていると考えられるからである。そしてかかるオーディオデータを暗号化部15に出力するということは、オーディオデータを二度重複して生成してしまうことになるからである。しかし、Ripper11から出力されるオーディオデータが著作権保護の対象外のパッケージコンテンツ（レガシーコンテンツ）に対応している場合、WaterMark Detector12は、WaterMarkを検出することなく、R

ipper 1 1 が出力したオーディオデータをそのまま暗号化部 1 5 に出力する。これにより、レガシーコンテンツについては、WaterMarkが存在しなくても、録再型PD 3 内部に取り込まれるのである。

#### 【0020】

信号ソースチェッカー 1 3 は、信号入力端子 9 のうち、アナログモノラルタイプの入力端子を介して録再型PD 3 内部に入力されてくる音声信号の正当性を判定するものである。具体的にいうなら、信号ソースチェッカー 1 3 は入力されてくる音声信号がアナログモノラルタイプであり、帯域制限されたものであるか否かを判定する。該当する場合、Ripper 1 4 にこの音声信号を出力する。入力されてくる音声信号がステレオタイプである場合、またはモノラルタイプであるが帯域制限が無い場合、信号入力端子 9 に不正なマイクが接続され、これから音声信号が順次入力されていると考えられるので、これらの場合には、音声信号をRipper 1 4 に出力しない。

#### 【0021】

Ripper 1 4 は、Ripper 1 1 と同一構成であり、信号ソースチェッカー 1 3 が出力したアナログ信号を圧縮符号化して暗号化部 1 5 に出力する。

暗号化部 1 5 は、録音操作がユーザインターフェイス部 8 に対して行われ、Ripper 1 4 又はWaterMark Detector 1 2 からオーディオデータが出力されれば、このオーディオデータについて固有の暗号鍵を生成し、暗号鍵を用いてオーディオデータを暗号化して暗号化オーディオデータを得る。

#### 【0022】

録再制御部 1 6 は、録音操作がユーザインターフェイス部 8 に対して行われ、暗号化部 1 5 から暗号化されたオーディオデータが出力されれば、暗号化部 1 5 から出力された暗号化オーディオデータをA0Bとしてユーザデータ領域 6 に書き込む。再生操作がユーザインターフェイス部 8 に対して行われれば、SDメモリカード 2 のユーザデータ領域 6 からA0Bを読み出して、復号化部 1 8 に出力する。

#### 【0023】

セキュアR/W部 1 7 は、録音操作がユーザインターフェイス部 8 に対して行われ、暗号鍵が暗号化部 1 5 から出力されれば、出力された暗号鍵と、「1」に設

定されたMPFと、このSDメモ리카ード2においてA0Bを一意に特定するContent-IDとを含むTKEをプロテクト領域7に書き込む。また再生操作がユーザインターフェイス部8に対して行われた場合は、プロテクト領域7からTKEを読み出し、TKEに格納されている暗号鍵を、この再生に用いるべき暗号鍵であるとして復号化部18に設定する。

#### 【0024】

復号化部18は、再生操作がユーザインターフェイス部8に対して行われ、録再制御部16からA0Bが出力されれば、セキュアR/W部17から出力される暗号鍵を用いてこのA0Bを復号化して、オーディオデータを再生部19に出力する。

再生部19は、復号化部18から出力されたオーディオデータを再生する。

以上で録再型PD3についての説明を終え、続いてライセンス管理装置1の内部構成について説明する。図4は、ライセンス管理装置1の内部構成を示す図である。図4に示すように、ライセンス管理装置1はSDメモ리카ード2を接続することができるコネクタを有し、ユーザインターフェイス部20、ローカルストレージ21、セキュアR/W部22、Licensed Compliantモジュール23を備える。

#### 【0025】

ユーザインターフェイス部20は、ディスプレイ、キーボード、マウス等で構成され、SDメモ리카ード2からA0Bを取り込む旨の操作、又は、SDメモ리카ード2へとチェックアウトを行う旨の操作を受け付ける。取り込み操作にあたってユーザインターフェイス部20は、SDメモ리카ード2に記録されている全てのA0Bの一覧表示を行い、取り込むべきA0Bの指定をドラッグ操作により受け付ける。チェックアウト操作にあたってユーザインターフェイス部20は、ローカルストレージ21に記録されている全てのA0Bの一覧表示を行い、取り込み時の場合と同じく、取り込むべきA0Bの指定をドラッグ操作により受け付ける。

#### 【0026】

ローカルストレージ21は、SDMIプロテクトコンテンツと、RMIとの組みを複数格納することができる内蔵型ディスク装置である。これらSDMIプロテクトコンテンツのうち、一回以上チェックアウトがなされたものについては、チェックアウト許可回数がデクリメントされ、チェックアウト履歴情報が対応づけられてい

る。チェックアウト履歴情報とは、チェックアウトにおいてA0Bの記録先となったSDメモ리카ード2に割り当てられていたMedia-IDと、そのSDメモ리카ード2においてSDMIプロテクトコンテンツを一意に特定するContent-IDとの組みであり、LCM23がチェックインを行う場合に用いられる。

#### 【0027】

セキュアR/W部22は、SDメモ리카ード2からの取り込みが命じられた場合、プロテクト領域7からTKEを読み出して、TKEをLCM23に出力する。チェックアウトが命じられれば、TKEをプロテクト領域7に書き込む。

LCM23は、SDメモ리카ード2がライセンス管理装置1に接続され、SDメモ리카ード2からデータ取り込みを行う旨が指示された場合に、チェックイン及びMigrateを択一的に行い、またチェックアウトが指示された場合に、チェックアウトを行う。取り込みにあたってLCM23は、チェックインの許否より優先して、Migrateの許否を判定するという処理を行っている。Migrate、チェックイン、チェックアウト時におけるLicensed Compliantモジュール23の処理を、以下の(i) (ii) (iii)に項分けして説明する。

#### 【0028】

(i) SDメモ리카ード2が接続され、SDメモ리카ード2からの取り込み操作がユーザインターフェイス部20に対して行われた場合、Migrateの許否を判定する。そのため先ず初めにTKEをプロテクト領域7から読み出し、このTKEにおいてMPFが「1」に設定されているか、「0」に設定されているかを判定する。MPFが「1」に設定されている場合、Migrate処理を行う。Migrate処理においてLCM23は、SDメモ리카ード2のユーザデータ領域6からA0Bを読み出して、SDMIプロテクトコンテンツとしてローカルストレージ21に格納する。それと共に、セキュアR/W部22を介して暗号鍵をプロテクト領域7から読み出して、この暗号鍵を含むRMIを生成し、ローカルストレージ21に格納する。以上の過程を経て、SDメモ리카ード2に記録されていたA0Bは、ローカルストレージ21においてSDMIプロテクトコンテンツとして管理されることになる。その後、Content-ID、MPFを「0」で上書きし、SDメモ리카ード2のTKE内における暗号鍵を乱数で上書きする。暗号鍵が乱数で上書きされることにより、その暗号鍵に対応するA0Bは、再生

不能な状態となる。

【0029】

(ii) チェックインは、Migrateが許可されていないと判定された場合にのみ行われる。即ち、MPFが「0」に設定された場合、LCM23は、TKEからContent-IDを読み出し、Media-IDを読み出して、このMedia-IDとContent-IDの組みに一致するチェックアウト履歴情報がローカルストレージ21に存在するかを判定する。Content-ID-Media-IDの組みに一致するチェックアウト履歴情報が存在しない場合、他のライセンス管理装置でチェックアウトがなされたものと判定して、SDメモ리카ード2に格納されているAOBのチェックインを行わない。Content-ID-Media-IDに一致するチェックアウト履歴情報が存在する場合、ライセンス管理装置1がチェックアウトを行ったと判定し、チェックインを実行する。チェックインにあたってAOB及び暗号鍵をSDメモ리카ード2からローカルストレージ21に移動させてもよいが、この場合、AOBの読み出しと書き込みに時間がかかってしまう。そのため、一般にチェックインは以下に示すように簡易に行われる。つまり、そのチェックアウト履歴情報に対応するSDMIプロテクトコンテンツのRMIを復号化して、RMIからチェックアウト許可回数を取り出し、チェックアウト許可回数をインクリメントした後、RMIを暗号化し直す。それと共にSDメモ리카ード2のTKEにおいて格納されているMPF、Content-IDを「0」で上書きし、暗号鍵を乱数で上書きする。

【0030】

(iii) チェックアウトを行う旨の操作がユーザインターフェイス部20に対して行われれば、LCM23はSDMIプロテクトコンテンツに対応するRMIを復号化し、RMIからチェックアウト許可回数と、暗号鍵とを取り出す。チェックアウト許可回数については、デクリメントした後、RMIに書き戻す。そして取り出した暗号鍵を格納するためのTKEを生成し、このSDメモ리카ード2においてユニークなContent-IDを、このTKEに割り当て、このContent-IDと、暗号鍵とを含むTKEをプロテクト領域7に書き込む。この際、MPFに対しては何の更新も行わないので、「0」に設定されたままである。その後、SDメモ리카ード2からMedia-IDを読み出して、TKEにおけるContent-IDと、Media-IDとを対応づけてチェックアウト履歴情

報としてローカルストレージ21に格納する。

#### 【0031】

以上に説明したシステムの動作例について説明する。本システムの特徴は、録再型PD3がSDメモリカード2にA0Bを記録する際、MPFを設定することなので、MPFを設定せずにSDメモリカード2にA0Bを記録する場合と、MPFを設定してSDメモリカード2にA0Bを記録する場合とを対比する形で動作例の説明を行う。まずはMPFを記録しない場合の動作例について説明する。図5は、MPFを用いずにMigrateを行う場合の、動作例を示す図である。本システムにおいてCDに記録されたパッケージコンテンツの再生がCDプレーヤ5により開始されれば、録再型PD3はこの再生信号を圧縮符号化することにより、A0Bx1を得て、①に示すようにMPFと対応づけることなく、A0Bx1をSDメモリカード2に記録する。一方、ライセンス管理装置Y2は、自身が内蔵しているSDMIプロテクトコンテンツx2についてチェックアウトを行うことにより、②に示すように、SDメモリカード2にA0Bx2を記録したとする、このようにA0Bx1、A0Bx2が記録されれば、録再型PD3により記録されたA0Bと、ライセンス管理装置Y2により記録されたA0Bとの区別がつかない。これらのA0Bが記録されたSDメモリカード2がライセンス管理装置Y1に接続された場合、③、④に示すようにA0Bx1、A0Bx2に対応するSDMIプロテクトコンテンツx1、x2と、これらに対応するRMIX1、RMIX2とがライセンス管理装置Y1内に生成されることになる。A0Bx2については、既にライセンス管理装置Y2にRMIX2が存在しているのに、ライセンス管理装置Y1にも、RMIX2が生成されているので、A0Bx2については、権利が二重に管理されていることになる。

#### 【0032】

続いて、PDがCDのバックアップをとる際、ライセンス管理装置1がMPFを用いてMigrate処理を行う場合の動作例について説明する。図6、図7は、MPFを用いる場合の動作例を示す図である。図6においてCDプレーヤ5がCDの再生を行い、CDプレーヤ5から出力される音声信号を録再型PD3が圧縮符号化してA0Bを得れば、①に示すようにMPFを「1」に設定して、A0Bx1に対応づけてSDメモリカード2に記録する。一方、ライセンス管理装置Y2がチェックアウトを行う場合は、MPFについては何の設定も行わず、②に示すようにそのまま記録する。その結果、

ライセンス管理装置Y2のチェックアウトにより記録されたA0Bは、「0」に設定されたMPFとSDメモリカード2において対応づけられることになる。A0Bx1、A0Bx2が記録されたSDメモリカード2がライセンス管理装置Y1に接続されれば、ライセンス管理装置Y1は、③に示すように各A0BについてのMPFの設定を参照し、Migrate処理を行うべきか否かを判定する。A0Bx1についてはMPFが「1」に設定されているので、ライセンス管理装置Y1はMigrate処理が許可されていると判定する。従って、④に示すようにA0Bx1に対してRMIX1を生成し、A0Bx1をSDMIプロテクトコンテンツx1としてローカルストレージ21に読み込むことにより、Migrate処理を行う。その後、図7の⑤に示すようにMPFを「0」に更新し、⑥に示すようにA0Bx1を再生不能な状態とする。一方、A0Bx2についてもMPFを参照することによりMigrate処理が許可されているか否かを判定する。MPFが「0」に設定されているので、図6の⑦に示すようにライセンス管理装置Y1がMigrate処理を行わない。これにより、既にRMIが生成されているA0Bについては、重複してRMIが生成されることが回避されている。

#### 【0033】

続いて、複数のSDMIドメインのうち、1つのSDMIドメインの録再型PD3がA0BをSDメモリカード2に記録した場合、このA0BについてのMigrateがどのように行われるかについて説明する。図8の一例では、複数のSDMIドメインY1、Y2、Y3、Y4、Y5があり、このうち1つのSDMIドメインに含まれる録再型PD3がA0Bx1を「1」と設定されたMPFと対応づけてSDメモリカード2に記録した場合、複数ライセンス管理装置Y1、Y2、Y3、Y4、Y5の何れもが矢印MR1、MR2、MR3、MR4、MR5に示すようにこのA0Bx1に対してMigrateを実行することができる。つまり録再型PD3によって記録されたA0Bx1は、SDMIドメインY1、Y2、Y3、Y4、Y5何れのSDMIドメインのライセンス管理装置であっても行なえるのである。しかし、一旦このA0Bx1についてのMigrateが行われれば、このA0Bx1は再生不能な状態にされ、二度とMigrateは実行されない。また1つのSDMIドメインY4に含まれるライセンス管理装置1がチェックアウトによりA0Bx2をSDメモリカード2に記録したとしても、他のライセンス管理装置Y5は、如何なる場合でも、このA0Bx2に対するMigrateを実行しない。何故ならA0Bx2は「0」と設定されたMPFに対応づけられてSDメモリカード2に記録されて



いるので、録再型PD 3により記録されたA0Bx1と明確に区別されているからである。ライセンス管理装置Y1のチェックアウトにより記録されたA0Bの利用は、ライセンス管理装置Y1のチェックアウトにより記録されたA0Bx3のようにPDにより再生されるのみに留まる。

#### 【0034】

以上のように本実施形態によれば、MPFに、各A0BについてMigrateの要否が示されているので、これに従えば、MigrateはRMIが存在しないA0Bに対して、一回限り許可されることになる。よってRMIが既に存在するA0Bに対して、重複してRMIが生成されることはない。これにより、著作権の保護に反することなく、チェックアウトにより得られたA0Bと、PDにより得られたA0Bとを同じ記録媒体に記録することができる。

#### 【0035】

##### (第2実施形態)

第2実施形態は、SD-Audio規格に基づくデータ構造にて、TKE、A0Bを格納し、処理する場合の改良に関する。

第2実施形態におけるSDメモリカード2は、図9の物理構成を有するSDメモリカード2であるものとする。

#### 【0036】

図9は、SDメモリカード2における物理層の構成を示す図である。本図に示すように、SDメモリカード2の物理層は、システム領域101、Hidden領域102、プロテクト領域103、AKE処理部104、AKE処理部105、Ks復号化部106、Ks暗号化部107、ユーザデータ領域108からなる。本図と図2に示したSDメモリカード2の内部構成とを比較すると、ユーザデータ領域6に相当するのがユーザデータ領域108であり、プロテクト領域7に相当するのがプロテクト領域103である。

#### 【0037】

システム領域101は、Media-IDと、Media Key Block (MKB) とを格納した読出専用領域であり、ここに格納されたMKB、Media-IDを書き換えることはできない。SDメモリカード2が、録再型PD 3、ライセンス管理装置1を初めとする他の機

器と接続され、MKBとMedia-IDとが他の機器により読み出された場合、これらを読み出した他の機器が、MKB、Media-IDと、自身が所持しているデバイス鍵Kdとを用いて所定の演算を正しく行えば、他の機器は正しい暗号鍵Kmuを所持することができる。

#### 【0038】

Hidden領域102は、正解値となる暗号鍵Kmu、即ち、他の機器が正常なデバイス鍵Kdを用いて正常な演算を行なった場合、得られるべき暗号鍵Kmuを格納している領域である。

プロテクト領域103は、TKEを複数収録したファイル(図中のA0BSA1.KEY)を格納する領域である。

#### 【0039】

Authentication and Key Exchange (AKE) 処理部104、AKE処理部105は、機器とSDメモリカード2との間でチャレンジ・レスポンス型の相互認証を行って、相手側の正当性を認証し、相手側が不当であれば処理を中断するが、相手側が正当であれば機器とSDメモリカード2との間で暗号鍵(セッション鍵Ks)を共有する。機器による認証は3つのフェーズ(機器側で乱数を発生させ、得られた乱数をKmuを用いて暗号化して、チャレンジ値AとしてSDメモリカード2に送信するChallenge1フェーズ、SDメモリカード2側でこのチャレンジ値AをSDメモリカード2内のKmuを用いて復号化し、得られた値をレスポンス値Bとして機器に送信するResponse1フェーズ、機器側で保持していたチャレンジ値Aを機器側のKmuで復号化して、SDメモリカード2から送信されたレスポンス値Bと比較するVerify1フェーズ)からなる。

#### 【0040】

SDメモリカード2による認証は3つのフェーズ(SDメモリカード2で乱数を発生させ、得られた乱数をKmuを用いて暗号化して、この値をチャレンジ値Cとして機器に送信するChallenge2フェーズ、機器側においてこのチャレンジ値Cを機器内のKmuを用いて復号化し、得られた値をレスポンス値DとしてSDメモリカード2に送信するResponse2フェーズ、SDメモリカード2側で保持していたチャレンジ値CをSDメモリカード2側のKmuで復号化して、機器から送信されたレスポンス値Dと

比較するVerify2フェーズ) からなる。

#### 【0041】

この際、他の機器が不正な暗号鍵K<sub>mu</sub>を用いて相互認証を行えば、フェーズVerify1, 2において、チャレンジ値Aとレスポンス値Bとの不一致、チャレンジ値Cとレスポンス値Dとの不一致が判定され、相互認証が中断することとなる。逆に相手側の正当性が認証されれば、AKE処理部104、AKE処理部105は、上述したチャレンジ値Aと、チャレンジ値Cとの排他的論理和をとり、これをK<sub>mu</sub>にて暗号化することにより、セッション鍵K<sub>s</sub>を得る。

#### 【0042】

K<sub>s</sub>復号化部106は、SDメモリカード2と接続された他の機器から、プロテクト領域103に書き込むべきTKEであって、暗号化されたものが出力された場合、それらTKEがセッション鍵K<sub>s</sub>を用いて暗号化されているものとして、セッション鍵K<sub>s</sub>を用いることにより復号を行う。そうして復号により得られた暗号鍵、Content-IDが本来のTKEであるとして、プロテクト領域103に書き込む。

#### 【0043】

K<sub>s</sub>暗号化部107は、SDメモリカード2と接続された他の機器から、TKEを読み出す旨のコマンドが出力されると、セッション鍵K<sub>s</sub>を用いてプロテクト領域103に格納されているTKEを暗号化した後に、そのコマンドを発行した他の機器に出力する。

ユーザデータ領域108は、機器の正当性が認証されるか否かに拘らず、当該機器によりアクセスされる領域であり、暗号化されたA0B (図中のA0B001. SA1) と、再生制御情報を複数収録したファイル (SD\_Audio. TKM) が格納される。プロテクト領域103から読み出された暗号鍵が正しい値であれば、ここに格納されている暗号化されたA0Bは正しく復号されることとなる。プロテクト領域103に対するデータ読み書きには、K<sub>s</sub>復号化部106による復号化と、K<sub>s</sub>暗号化部107による暗号化とが伴うので、プロテクト領域103は、SDメモリカード2と接続している機器がAKEプロセスを正しく行った場合のみ、当該機器により正規にアクセスされることとなる。

#### 【0044】

続いて、SDメモ리카ード2のディレクトリ構成、ファイル構成について説明する。

図10は、SDメモ리카ード2におけるユーザデータ領域108、プロテクト領域103のディレクトリ構成、ファイル構成を示す図である。本図においてプロテクト領域103、ユーザデータ領域108のそれぞれにSD\_Audioディレクトリが設けられ、ユーザデータ領域108のSD\_Audioディレクトリには、8つのAOBを格納した8つのAOBファイル(AOB001.SA1、AOB002.SA1、AOB003.SA1、AOB004.SA1、…、AOB008.SA1)と、SD\_AUDIO.TKMとが配置されている。プロテクト領域103のSD\_Audioディレクトリには、AOBSA1.KEYが配置されている。AOBファイルのファイル名における“001”～“008”の番号は、AOB-IDである。AOBSA1.KEYに含まれる8つのTKEや、SD\_AUDIO.TKMに含まれる8つのTrack Information(TKI)にも、AOB-IDと同じ番号を示す#1、#2、#3、#4、…、#8の番号が割り当てられている。各AOBファイルを暗号化する際に用いた暗号鍵“EKey”は、AOB-IDと同一の番号を有する『TKE』に格納され、AOBを再生するための再生制御情報は、AOB-IDと同一番号を有する『TKI』に存在することとなる。

#### 【0045】

続いてTKEの内部構成について説明する。図11は、TKEの内部構成を示す図である。図11の破線h1に示すように、TKEは、『MPF』、7バイトの暗号鍵『EKEY』、『Availability Flag』、『Content ID』とからなる。尚、本実施形態におけるMPFは、第1実施形態におけるMPFと同一であって、録再型PDでAOBを記録した場合に限り“1”に設定されるものとする。

#### 【0046】

第2実施形態における『Content ID』は、Availability Flagと以下のように併用される。あるTKEに対応するAOBファイルが存在する場合、TKEについてのContent\_IDは“001”～“999”の何れかに設定される。あるTKEに対応するAOBファイルが存在しない場合、TKEについてのContent\_IDは“000”と設定される。更にTKEとAOBとが1対多で対応する場合、AOBに対応するTKEにおけるContent\_IDが、全て同一の値となる。一方Availability Flag及びMPFは、TKEとAOBとが1対1で対応する場合“1”に設定される。AOBとTrackとが1対多で対応する場合、多のTKEのうち、

先頭のもののAvailability Flag及びMPFが“1”に設定される。先頭以外のTKEのAvailability Flag及びMPFは“0”に設定される。Content\_IDが“000”ではなく、Availability Flagが“0”に設定されていれば、同一のContent\_IDを有するA0Bが複数存在し得るから、これを手掛かりに同一のContent\_IDを有するTKEを検出する。そうして1つのContent\_IDに対応する複数のA0Bを特定するというサーチ処理が可能となる。

#### 【0047】

続いて、図10に示した8つのA0Bファイルに収録される8つのA0Bが、どのようなパッケージコンテンツに対応するかを示すかについて説明する。図12は、A0Bと、パッケージコンテンツの対応関係の一例を示す図である。

本図の第3段目は、本図における8つのA0Bがどのようなパッケージコンテンツに対応するかを示す図である。本図における8つのA0Bは、Content.A、Content.B、Content.C、Content.D、Content.Eに対応するものとする。第2段目は、第3段目のコンテンツがどのような単位で分割されるかを示し、第1段目は、図10に示した8つのA0Bファイルに収録される8つのA0Bを示す。破線AS1、AS2、AS3……AS7、AS8は、コンテンツの分割部分と、A0Bとの対応関係を示す。パッケージコンテンツA、B間、パッケージコンテンツB、C間、パッケージコンテンツC、D間、パッケージコンテンツD、E間には無音区間が存在しており、本図におけるA0Bは、この無音区間を境界として生成されている。

#### 【0048】

A0B#4は、30.6分という時間にて再生されるコンテンツ(Content.D)の先頭部分であり、8.4分という再生時間にて再生される。A0B#5、A0B#6はContent.Dの中間部分であり、8.4分という再生時間、A0B#7は、Content.Dの終端部分であり、5.4分という再生時間にて再生される。このように30.6分という再生時間を有するコンテンツは、(8.4分+8.4分+8.4分+5.4分)という単位で分割され、各A0Bに含まれていることがわかる。この図からも理解できるように、A0Bファイルに含まれる全てのA0Bは、再生時間長が8.4分という時間長以内に収められていることがわかる。

#### 【0049】

図13は、TKIと、A0Bファイルと、TKEとの相互関係を示す図である。図13の第1段目における四角枠はSD\_AUDIO.TKMを示し、第2、第3段目は図10に示した8つのA0Bファイルを示す。第1段目のSD\_Audio.TKMに含まれる8つのTKIを示す。各TKIには、TKIを特定する番号“#1”、“#2”、“#3”、“#4”、……“#7”、“#8”がTKI-IDとして割り当てられている。各TKIは、TKI-IDと同じ番号がA0B-IDとして割り当てられたA0Bファイルと対応している。各TKEには、TKEを特定する番号“#1”、“#2”、“#3”、“#4”……“#7”、“#8”が付与されている。各TKEは、同じ番号がA0B-IDとして付与されたA0Bファイルと対応している。この点に注意して、図13を参照すれば、TKI#1とTKE#1とがA0B001.SA1に対応していて、TKI#2とTKE#2とがA0B002.SA1、TKI#3とTKE#3とがA0B003.SA1、TKE#4とTKI#4とがA0B004.SA1に対応していることがわかる。本図における矢印TA1、TA2、TA3、TA4……は、各TKIがどのA0Bファイルと対応しているかを示し、本図における矢印KA1、KA2、KA3、KA4……は、各TKEがどのA0Bファイルと対応しているかを示す。

#### 【0050】

第4段目における8つの枠は、8つのTKEを示す。この8つのTKEは、5つのEKey（EKey#1、EKey#2、EKey#3、EKey#4、EKey#5）と、5つのContent-ID（001、002、003、004、005）と、8つのAvailability Flag、8つのMPFを収録している。本図におけるTKEのうち、Content.Dと1対多の関係で対応するTKE#4～#7については、TKE#4のMPF及びAvailability Flagが「1」に設定され、残りのTKE#5、#6、#7についてのMPF及びAvailability Flagは「0」に設定される。またTKE#4にのみTitle Key#4が書き込まれており、残りのTKE#5、#6、#7については乱数が書き込まれている。

#### 【0051】

図14を参照しながら、A0Bの再生制御情報たるTKIについて説明する。図14を参照すると各TKIは、破線の引き出し線h2に示すように、Track\_General\_Information (TKGI)、アーティスト名、アルバム名、編曲者名、プロデューサ名等、TKIに固有なテキスト情報が記述されるTrack\_Text\_Information\_Data\_Area (TKTXTI\_DA)、8.4分という再生時間を上限としたタイムサーチテーブル (Track\_Time\_Search\_Table (TKTMSRT)) からなる。

## 【0052】

TKIは、破線の矢印h3に示すように、『TKI\_ID』『TKIN』『TKI\_BLK\_ATR』『TKI\_LNK\_PTR』『ISRC』『BIT』を含む。

『TKI\_ID』には、TKIを一意に識別できるID(本実施形態では2バイトの'A4'というコード)が記述される。

『TKIN』には、1から999までの範囲のTKI番号が記述される。

## 【0053】

『TKI\_BLK\_ATR』には、TKIについての属性が記述される。図13の一例では、それぞれのTKIについてのTKI\_BLK\_ATRがどのように設定されているかについて説明する。各TKIにおけるTKI\_BLK\_ATRを参照すれば、TKI#1とA0B001. SA1との組み、TKI#2とA0B002. SA1との組み、TKI#3とA0B003. SA1との組み、TKI#8とA0B008. SA1との組みは、それぞれが独立したTrackに対応しているので、TKI#1、TKI#2、TKI#3、TKI#8のTKI\_BLK\_ATRは、『Track』と設定されている。TKI#4におけるTKI\_BLK\_ATRは『Head\_of\_Track』と設定され、TKI#7におけるTKI\_BLK\_ATRは『End\_of\_Track』と、TKI#5、TKI#6は『Midpoint\_of\_Track』と設定されていることがわかる。このことは、TKI#4と対応関係を有するA0B004. SA1はTrackの先頭部、TKI#5、TKI#6と対応関係を有するA0B005. SA1及びA0B006. SA1はTrackの中間部、TKI#7と対応関係を有するA0B007. SA1はTrackの終端部であることを意味する。

## 【0054】

このTKI\_BLK\_ATRを設定することにより、複数のTrackのうち、任意の2つを1つのTrackに統合するという統合編集、1つのTrackを複数に分割するという分割編集が容易に行なえることとなる。Trackの統合を行う際の、TKIの更新について説明する。

図15は、2つのTrackを1つに統合する場合にTKIがどのように設定されるかを示す図である。図13において、Track.CとTrack.Eとを1つのTrackに統合するという編集操作を操作者が希望しているものとする。これらTrack.C、Track.Eに対応するAOBがA0B003. SA1、A0B008. SA1に収録されており、それらがTKI#3、TKI#8に対応づけられているので、これらTKI#3及びTKI#8のTKI\_BLK\_ATRの書き換えが行われる。図15にTKIのTKI\_BLK\_ATRの書き換え後の状態を示す。図13におい

てTKI#3、TKI#8のTKI\_BLK\_ATRはTrack. C、Track. Eと記載されているが、図15では、TKI#3のTKI\_BLK\_ATRは『Head\_of\_Track』に書き換えられ、TKI#8のTKI\_BLK\_ATRは『End\_of\_Track』に書き換えられている。このように、TKI\_BLK\_ATRが書き換えられることにより、TKI#3、TKI#8、AOB003. SA1、AOB008. SA1、TKE#3、TKE#8は、Track. Cという1つのTrackとして扱われる。この際、AOB003、AOB008に対応するTKE#3、TKE#8には、元のContent-IDであるContent-ID=003、Content-ID=005が格納される。またTKE#3、TKE#8には、元の暗号鍵であるEkey3、Ekey5、「1」に設定されたMPF、「1」に設定されたAvailability Flagが格納される。

#### 【0055】

Trackの分割を行う際のTKIの更新について説明する。図16は、1つのTrackを2つのTrackに分割する場合を想定した図である。図13において、Track. CをTrack. C-Track. Fという2つのTrackに分割するという編集を操作者が希望しているものとする。この場合、Track. Cを構成するAOB#3を分割して新たなAOBを得る。そして、001~008の番号が割当済みなので、未割当番号009を分割により得られたAOBに割り当てて、AOB009を得る。その後、このAOB009. SA1に対応するTKI#9と、TKE#9とを生成して図16の状態となる。Title Key Entry#9には、AOB003に割り当てられていたContent-ID=003と、AOB003の暗号化に用いられたEKey3と、「0」に設定されたMPFと、「0」に設定されたAvailability Flagとが格納される。以上でTKI\_BLK\_ATRについての説明を終え、TKIの構成要素についての説明を再開する。

#### 【0056】

『TKI\_LNK\_PTR』には、当該TKIのリンク先のTKIについてのTKINが記述される。図13において矢印TL4、TL5、TL6に示すように、Track. Dを構成する4つのAOBファイルに対応するTKI#4、TKI#5、TKI#6、TKI#7は、各TKI\_LNK\_PTRが次のTKIを指示するように設定されている。

『ISRC』には、TKGIにおけるISRC (International Standard Recording Code) が記述される。

#### 【0057】

『ブロック情報テーブル (BIT)』は、AOBのうち、どの部分を有効部分とするか



を管理するテーブルである。このBITを更新することにより、A0Bの先端部分、終端部分をカットすることが可能となる。

続いて第2実施形態に係る録再型PD3、ライセンス管理装置1の構成について説明する。第2実施形態に係る録再型PD3、ライセンス管理装置1が第1実施形態に示したものと異なるのは、録再型PD3及びライセンス管理装置1に備えられていたセキュアR/W部26が、図17の内部構成を有する点である。セキュアR/W部14は、録再型PD3がSDメモ리카ード2と接続された際、SDメモ리카ード2とMKB、Media-IDを用いたAKEプロセスと、セッション鍵Ksを用いたデータの暗号化、復号化を行うものであり、セキュアR/W部26は、ライセンス管理装置1がSDメモ리카ード2と接続された際、SDメモ리카ード2とMKB、Media-IDを用いたAKEプロセスと、セッション鍵Ksを用いたデータの暗号化、復号化とを行うものである。

#### 【0058】

図18に示すようにセキュアライト部31は、MKB処理部41、ID処理部42、AKE処理部43、Kmu暗号化部44、Ks暗号化部45からなる。

MKB処理部41は、SDメモ리카ード2のシステム領域に格納されているMKBと、録再型PD3、ライセンス管理装置1の製造メーカーにより付与されたデバイス鍵Kdとを読み出し、これらを用いて所定の演算を行うことにより、56ビットの暗号鍵KmをID処理部42に出力する。

#### 【0059】

ID処理部42は、MKB処理部41から56ビットの暗号鍵Kmが出力されれば、SDメモ리카ード2のシステム領域からMedia-IDを読み出して、所定の演算を行うことにより、64ビットの演算結果を算出し、そのうち下位56ビットを暗号鍵Kmuとして、AKE処理部43及びKmu暗号化部44に出力する。

AKE処理部43は、ID処理部42により算出された暗号鍵Kmuと、SDメモ리카ード2側の暗号鍵Kmuとを用いたAKEプロセスを行う。その結果として得られた56ビットのセッション鍵KsをKs暗号化部45に出力する。

#### 【0060】

Kmu暗号化部44は、SDメモ리카ード2に記録すべきA0BSA1.KEYに含まれるTKE

を、ID処理部42が出力した暗号鍵Kmuを用いて暗号化してKs暗号化部45に出力する。

Ks暗号化部45は、AKE処理部43から出力された56ビットのセッション鍵Ksを用いて、Kmu暗号化部44により暗号化されたA0BSA1. KEYに含まれるTKEを更に暗号化して、SDメモリカード2に出力し、プロテクト領域103に書き込ませる。

#### 【0061】

一方セキュアリード部32の内部構成は、図19に示す通りであり、MKB処理部51、ID処理部52、AKE処理部53、Ks復号化部54、Kmu復号化部55からなる。

MKB処理部51は、SDメモリカード2が録再型PD3、ライセンス管理装置1に接続されると、システム領域101からMKBを読み出し、デバイス鍵Kdを用いて読み出されたMKBに対して所定の演算を行うことにより、56ビットの暗号鍵Kmを得る。

#### 【0062】

ID処理部52は、接続されたSDメモリカード2のシステム領域101からMedia-IDを読み出し、MKB処理部51により算出された暗号鍵Kmと、読み出されたMedia-IDとを用いて所定の演算を行い、64ビットの演算結果を得て、そのうち下位56ビットを暗号鍵Kmuとして、AKE処理部53とKmu復号化部55とに出力する。

AKE処理部53は、ID処理部52により出力された暗号鍵Kmuを用いて、SDメモリカード2におけるAKE処理部105とAKEプロセスを行い、その結果である56ビットのセッション鍵KsをKs復号化部54に出力する。

#### 【0063】

Ks復号化部54は、プロテクト領域103に暗号化された状態で格納されているA0BSA1. KEY (TKEを含む)を読み出し、AKE処理部53が出力した56ビットのセッション鍵Ksを用いて復号する。そしてその結果をKmu復号化部55に出力する。

Kmu復号化部55は、ID処理部52により算出された56ビットの暗号鍵Kmuを用いて、A0BSA1. KEYにおけるTKEを復号化する。

#### 【0064】

以上のように、SDメモリカード2のプロテクト領域103に対するアクセスは、セッション鍵Ks、Kmuを用いた暗号化、復号化、AKEプロセスが伴うので、不正な機器によるアクセスは排除され、録再型PD3、ライセンス管理装置1のような正当な機器のみにより、正当に読み書きされることとなる。

続いて図19に示したセキュアR/W部22を介して、ライセンス管理装置1がMigrateを行う際の動作例を図20を参照しながら説明する。

#### 【0065】

図20は、図13に示した8つのA0B及び8つのTKEについて、Migrate処理が行われる様子を示す図である。図13に示した8つのTKEに対してMigrate処理が行われれば、図13に示したA0B#1～#3、A0B#8は、矢印MY1、MY2、MY3、MY8に示すようにそれぞれSDMIプロテクトコンテンツA、B、C、Eとしてローカルストレージ21に格納される。1つのパッケージコンテンツに対応したA0B#4～#7は、矢印MY4、MY5、MY6、MY7に示すようにSDMIプロテクトコンテンツDとしてローカルストレージ21に格納される。その後、矢印RY1、RY2、RY3、RY4、RY5に示すように、これら5つのContent A～Content Eについて権利管理情報(RMI) A～Eが生成され、この中に“3回”というチェックアウト許可回数と、TKE#1～#5に格納されていたEKEY#1～#5とが矢印ME1、ME2、ME3、ME4、ME5に示すように格納されている。そして8つのTKEのそれぞれのMPF及びAvailability Flagが「0」に設定され、Content-IDが“000”に設定されて、TKE#1～#5におけるEKEYは乱数で上書きされる。これによりSDメモリカード2におけるA0B#1～A0B#8は、再生不能な状態となる。図20のようなMigrateを行った後のローカルストレージ21の格納内容について以下説明する。

#### 【0066】

図15のように、Track同士の統合操作が行われている場合、LCM23は以下のようにしてMigrateを行う。まず初めにLCM23は、TKI\_BLK\_ATRが共通のTrackの先頭部分(Head of Track)、後半部分(End of Track)を示しているにも拘らず、TKEにおけるContent-IDが、異なるものを探し出す。Content-IDが異なっているにも拘らず、TKI\_BLK\_ATRが1つのTrackの先頭部分、後半部分を示しているものは、本来別々のTrackであったものが後発的な編集により、1以上のTrackに統合されたものと考えられる。

## 【0067】

同一のContent-IDを有するTrackの先頭部分、Trackの後半部分を探し出せば、これら先頭部分、後半部分を元の1つのTrackに戻してからMigrateを行う。即ち、図16の一例では、同一のContent-ID=003, 005を有するTrackCの先頭部分 (Head of TrackC)、TrackCの後半部分 (End of TrackC) を探し出し、これら先頭部分、後半部分をTrackC, TrackEに戻してからMigrateを行う。

## 【0068】

図16のように1つのTrackが2以上のTrackに分割されている場合は、以下のようにして、元のTrackに戻してからMigrateを行う。先ず初めにLCM23は、各TrackのTKEを参照して、TKI\_BLK\_ATRが別々のTrackを示しているにも拘らず、TKEにおけるContent-IDが、同じものを探し出す。TKI\_BLK\_ATRが別々のTrackを示しているにも拘らず、TKEにおけるContent-IDが、同じものは、本来1つのTrackであったものが後発的な編集により、2以上のTrackに分割されたものと考えられる。

## 【0069】

同一のContent-IDを有するTrackを探し出せば、これらTrackを元の1つのTrackに戻してからMigrateを行う。即ち、図16の一例では、同一のContent-ID=003, 003を有するTrackC、TrackFを探し出し、これらをTrackCに戻してからMigrateを行う。

BITの設定により、A0Bの先頭部分、後半部分が部分的にカットされている場合は、BITの設定を元の状態に戻してからMigrateを行う。

## 【0070】

本実施形態にかかるLCM23は、統合、分割、部分カットという操作がTrackに対して行われた場合でも、これをパッケージコンテンツと等価な状態に戻してからMigrateを行うので、図15、図16の状態にあった複数のA0B、TKE、TKIをLCM23は、図13に示した状態、即ち、CDに記録されていた状態と等価な状態で、管理することができる。これにより、PDに記録されてからLCMによりMigrateがなされるまでに編集が行われたとしても、著作物の同一性が害されることはない。

## 【0071】

図21は、ローカルストレージ21のディレクトリ構成、ファイル構成を示す図である。本図に示すようにローカルストレージ21には、一般のアプリケーションプログラムであってもアクセスすることができるユーザ領域と、LCM23のみがアクセス可能であり、他のアプリケーションプログラムのアクセスは禁止されるセキュア領域とを備える。ユーザ領域のルートディレクトリは、SDMIプロテクトコンテンツ格納用のディレクトリであるPackageディレクトリが存在する。このPackageディレクトリは、SDMIプロテクトコンテンツが格納されるディレクトリであり、ここに図20に示した5つのパッケージが格納される。これら5つのパッケージはそれぞれ、SDMIプロテクトコンテンツと、RMIの組みとを格納している。

#### 【0072】

ユーザ領域には、パッケージ管理テーブルが配置される。パッケージ管理テーブルは、パッケージについての『インデックス番号』と、パッケージが格納されているファイルの所在を示す『ファイルパス』と、パッケージに相当するコンテンツのアーティスト名、タイトルを示す『コンテンツ紹介情報』とからなる。ユーザは、このパッケージ管理テーブルを参照することにより、どのコンテンツがどのディレクトリにどのようなファイル名で格納されているかを知ることができる。このパッケージ管理テーブルは、ユーザインターフェイス部20がローカルストレージ21に格納されているSDMIプロテクトコンテンツを一覧表示する際に用いられる。

#### 【0073】

続いてセキュア領域について説明する。セキュア領域は、課金情報等、ユーザによる改竄を禁ずるべき情報が格納される領域であり、各コンテンツについてのチェックアウト履歴情報とからなるチェックアウト履歴情報テーブルはここに格納される。この図21の状態ではチェックアウトが未だ実行されていないので、チェックアウト履歴情報は空白になっている。続いて5つのSDMIプロテクトコンテンツContent.A～Content.Eについて、チェックアウトが行われる様子について説明する。図22は、チェックアウトにより、SDメモ리카ード2に8つのA0Bと、8つのTKEとが格納される様子を示す図である。ユーザによりチェックアウトが命

じられると、矢印TY1, TY2, TY3, TY8に示すようにContent. A、Content. B、Content. C、Content. Eはそれぞれ単体のA0B#1、A0B#2、A0B#3、A0B#8としてSDメモリカード2に記録される。Content. Dは矢印TY4, TY5, TY6, TY7に示すようにA0B#4～A0B#7としてSDメモリカード2に記録される。その後、A0B#1～A0B#8に対応するTKE#1～#8を生成し、MPFを「0」としたまま、Title Key#1～#5と、001～005のContent-IDと(矢印CY1, CY2, CY3, CY4, CY5参照)、Availability Flagとを記録する。その後、RMI内のチェックアウト許可回数をデクリメントして2回とする。このMedia-ID'AA1'と、Content-ID001～005とを対応づけたチェックアウト履歴情報を生成して、ローカルストレージ21に格納する。図23は、チェックアウトが実行された後のローカルストレージ21の格納内容を示す図である。図21との相違点は、チェックアウト許可回数が3回から2回にデクリメントされ、セキュア領域にチェックアウト履歴情報A～Eが生成されている点である。

#### 【0074】

以上に説明した第2実施形態に係るライセンス管理装置1の動作をフローチャートを参照しながら説明する。図24は、第2実施形態に係るLCM23の処理手順を示すフローチャートである。ステップS1においてSDメモリカード2からMedia-IDを読み出し、ステップS2では、SDメモリカード2のファイルエントリを参照して、SDメモリカード2に記録されている複数A0Bの一覧表示を行う。SDメモリカード2に記録されているA0Bは、チェックアウトにより記録されたA0Bであっても、録再型PD3により記録されたA0Bであっても、区別することなく一律に表示されることになる。尚、この際MPFを読み込み、Migrateが許可されているA0Bのみ一覧表示を行っても良い。このようにして表示された複数のA0Bに対して、取り込むべきA0Bについての指定を操作者から受け付ける。ドラッグ指定等によりライセンス管理装置1に取り込むべきA0Bが指定されれば、ステップS3、ステップS4を繰り返し条件とするループ処理に移行する。本ループ処理は、ステップS2において指定されたA0Bのそれぞれに対応するTKEについて、ステップS5～ステップS25を繰り返すものである。以降1つのTKEを処理対象として着目して説明を行う。

#### 【0075】

ステップS 5においてTKEにContent-IDが000であるか否かを判定する。Content-IDが000であれば、そのTKEに対応するA0Bが存在しないので、次のTKEを処理対象とすべく(A)記号を介してステップS 4に移行する。Content-IDが000でなければ、Migrateを行うべきTKEである可能性がある。そのためステップS 6に移行し、MPFが0であるか1であるかを判定する。録再型PD 3により記録されたTKEは、MPFが「1」に設定され、ライセンス管理装置1により記録されたTKEと明確に区別されているので、MPFが「1」であればステップS 7に移行する。ステップS 7においてAvailability Flagが「1」であるか「0」であるかの判定を行う。Availability Flagが「1」であることは、処理対象たるTKEがパッケージコンテンツと1対1の比率で対応しているTKEであるか、又は、パッケージコンテンツと1対多の比率で対応している複数TKEのうち、先頭のもの(図13の一例でいえばTKE#4)であることを意味する。Availability Flagが「1」なら、ステップS 8に移行し、RMIを有する管理パッケージを生成する。その後、ステップS 9においてTKEに対応するA0Bを読み出して、SDMIプロテクトコンテンツとして管理パッケージに格納する。ステップS 10においてSDメモリカード2のTKEからEKeyを読み出して、管理パッケージのRMIに格納する。ステップS 11においてRMIに3回と設定されたチェックアウト許可回数を格納し、公開鍵で暗号化する。以上の過程を経て、SDメモリカード2に記録されたA0Bは、SDMIプロテクトコンテンツとしてライセンス管理装置1の管理下におかれることになる。続くステップS 12では、TKEにおけるAvailability Flag、MPFを「0」に設定し、Content-IDを「000」に上書きする。ステップS 13においてLicensed Compliantモジュール23は、TKEにおけるEKeyを乱数で上書きする。Title Keyが上書きされることにより、A0Bは再生不能な状態に設定されることになる。

#### 【0076】

ステップS 7においてAvailability Flagが「0」とであると判定された場合、処理対象たるTKEは、パッケージコンテンツと1対多に対応する複数TKEのうち、先頭以外のもの(TKE#5, #6, #7)と考えられる。そのため、処理対象のTKEはステップS 14において、TKEのContent-IDが直前のTKEのContent-IDと同一であるか否かを判定し、もし同一ならば、ステップS 15において、A0Bを読み出して、直前

に生成された管理パッケージに追加して、その後、ステップS 1 6においてそのContent-IDを000で上書きする。

#### 【0077】

MPFが「0」に設定され、Migrateが許可されていない場合、ステップS 1 6からステップS 1 7に移行して、チェックインの許否についての判定を行う。即ちContent-ID-Media-IDの組みに一致するチェックアウト履歴情報がローカルストレージ2 1に存在するか否かを判定する。このチェックアウト履歴情報がローカルストレージ2 1に無ければ、このTKEがこのライセンス管理装置1のチェックアウトにより記録されたものでないことは明らかなので、チェックインを行うことなく、(A)記号を介してステップS 4に移行する。チェックアウト履歴情報が存在すれば、ステップS 1 8においてAvailability Flag=1であるか否かを判定する。先にも述べたように、Availability Flagが「1」であるということは、処理対象となるTKEは、パッケージコンテンツと1対1の比率で対応しているTKE、又は、1対多の比率で対応しているTKEのうち先頭のTKE（図1 3の一例でいえばTKE #4）である。処理対象がこれらに該当するなら、ステップS 1 9において、公開鍵を用いてContent-IDに対応するSDMIプロテクトコンテンツのRMIを復号化し、ステップS 2 0においてRMIに含まれるチェックアウト許可回数をインクリメントして、ステップS 2 1においてContent-IDに対応するSDMIプロテクトコンテンツのRMIを暗号化する。ステップS 2 2において、Content-IDとMedia-IDとの組みを含むチェックアウト履歴情報を、チェックアウト履歴情報テーブルから削除して、ステップS 2 3においてAvailability Flagを0で上書きし、Content-IDを000で上書きし、ステップS 2 4においてEKeyを乱数で上書きする。

#### 【0078】

ステップS 1 8において Availability Flagが0であると判定された場合、この処理対象たるTKEは、1つのパッケージコンテンツに1対多の比率で対応する複数TKEのうちの先頭以外のものであり、このTKEにおいて有効なのはこのContent-IDのみなので、ステップS 2 5においてContent-IDを000で上書きする。

以上のように本実施形態によれば、接続された機器の正当性が判明しない限りアクセスされ得ないプロテクト領域1 0 3にTKEを格納しておくので、MPFの改竄



を防止することができる。よって、コンテンツの著作権保護に万全の配慮を払いながら、録再型PD 3により記録されたAOBについてのMigrateを実現することができる。

#### 【0079】

##### (第3実施形態)

SDMIには、Migrateと類似した概念として、MOVEというものがあり、第3実施形態は、このMOVEの対象となるAOBと、MigrateすべきAOBとを共通のSDメモリカード2に記録する場合の改良に関する。先ず初めにMOVEと、第1、第2実施形態で説明したMigrateとがどのように違うのか以下に簡単に説明する。

#### 【0080】

MOVEは、電子音楽配信により得られたAOBを対象とするものであり、AOBは、チェックアウト許可回数を含むRMIが付されて、MOVE許可回数に示された範囲でSDMIドメイン間を転々とする。

これに対してMigrateの対象となるべきAOB (MigrateすべきAOB) は、MPFが付されてPDからSDMIドメインへと一回限り移転する。

#### 【0081】

このことから、MigrateすべきAOBがMOVEすべきAOBと決定的に異なるのは、MigrateすべきAOBは、RMIがなく、SDMIドメインへの受け入れを求めている状態であるということ、つまり、SDMIドメインでの保護を求めるまでの過渡的な状態であることといえる。MigrateすべきAOBをMOVEすべきAOBと区別するため、本実施形態ではRMIが既にSDメモリカード2に記録されているAOBについてもMPFを「0」に設定しておく。図25は、第3実施形態におけるMPFの設定例を示す図である。

#### 【0082】

以上のように本実施形態によれば、MPFを「0」に設定することにより、MOVEを行うべきAOBに対して、Migrateが行われることを避けることができる。

尚、第1、第2、第3実施形態に開示されるデータ構造、各種処理は、以下の国際公開番号公報に基づくものであり、より詳細な技術事項については、これらの公報を参照されたい。

#### 【0083】

WO 00/65602号公報 2000年11月2日 WO 00/74054号公報 2000年12月7日

WO 00/74059号公報 2000年12月7日 WO 00/74060号公報 2000年12月7日

WO 01/16821号公報 2001年 3月8日

また本発明はその要旨を逸脱しない範囲で変更実施することができる。代表的な変更実施の形態として、以下（A）～（G）のものがある。

#### 【0084】

（A）CDに記録されたパッケージコンテンツを圧縮符号化することにより得られたオーディオデータを対象として説明を行ったが、DVD-Audioやカセットテープに記録されたパッケージコンテンツを圧縮符号化することにより得られたオーディオデータを対象としてよいことはいうまでもない。

また「1」がオンでMigrateを許可し、「0」がオフでMigrateを許可しないというMPFの設定は一例であり、「0」がオンでMigrateを許可し、「1」がオフでMigrateを許可しないという設定にしてもよい。

#### 【0085】

（B）録再型PD3がスクリーニング部10を備え、パッケージコンテンツの圧縮符号化を行ったが、ライセンス管理装置1自身がパッケージコンテンツの圧縮符号化を行ってよいことはいうまでもない。

（C）録再型PD3は、コンポーネントステレオ、携帯電話、PDA(Personal Digital Assistant)で実現されてもよい。またCDやDVD-Audioを再生する再生装置と、録再型PD3とを一体構成として、コンポタイプの録再型PDとしてもよい。ライセンス管理装置1はパーソナルコンピュータで実現されとしたが、内蔵記憶装置を持つラジカセ、コンポ、STB(Set Top Box)などで実現されてもよい。

#### 【0086】

（D）第1実施形態、第2実施形態においてRMIには、暗号鍵とチェックアウト許可回数とが格納されていたが、他の情報が格納されていてよいことはいうまでもない。かかる情報には、パソコン(ライセンス管理装置1)でのSDMIプロテクトコンテンツの再生を許可するか否かを示す情報(PC再生可否情報)、再生回数を制限する場合の再生回数情報等がある。

#### 【0087】

(E) 本実施形態において機能ブロックを用いて説明した手順や、フローチャートを参照して説明した手順(図24)を実行形式プログラムにより実現し、これを記録媒体に記録して流通・販売の対象にしても良い。このような記録媒体には、ICカードや光ディスク、フレキシブルディスク等があるが、これらに記録された機械語プログラムは汎用コンピュータにインストールされることにより利用に供される。この汎用コンピュータは、インストールした機械語プログラムを逐次実行して、第1、第2実施形態に示したライセンス管理装置1、記録再生装置の機能を実現する。

【0088】

(F) 第1実施形態、第2実施形態においてMigrateの対象となるデータはオーディオデータであったが、動画データ等、他のストリーム形式のデータであってもよい、この場合、PDが動画配信サービス等により動画のストリームデータを得た場合、このストリームデータを「1」に設定されたMPFと共にSDメモリカード2に記録する。ライセンス管理装置1は、SDメモリカード2におけるMPFが「1」に設定されていることを確認した上で、Migrateを行うのである。これによりストリームデータは、RMIと共にライセンス管理装置1内部で管理される。その後、このストリームデータについてのチェックアウトを行う場合、ライセンス管理装置1は、「0」に設定されたMigrateと共に、ストリームデータをSDメモリカード2に記録する。

【0089】

(G) 第1実施形態においてWaterMark Detector 12は、WaterMarkをオーディオデータから検出した場合、オーディオデータからWaterMarkを取り除いたが、WaterMarkを書き換えてもよい。即ち、WaterMark Detector 12は、WaterMarkを検出した際、このWaterMarkを解読する。この解読結果が「コピー許可」であれば、このWaterMarkを、「コピー禁止」に書き換えて、暗号化部15に出力するのである。

【0090】

(産業上の利用可能性)

著作権保護のためのSDMIシステムにおける1つのSDMIシステムにおいて、CDに

記録されたパッケージコンテンツの圧縮符号化をPDが行い、ライセンス管理装置1が安全にこれを取り込むことができるので、著作権者の利益と、ユーザの利便性との両立が可能となる。よって、ライセンス管理装置1や録再型PD3の製造に携われるメーカー各社は、著作権の利益と、ユーザの利便性とを両立させた商品価値が高いライセンス管理装置1、SDメモリカード2、録再型PD3を製品化して、市場に投入することができ、機器製造産業を活性化させることができる。

【図面の簡単な説明】

【図1】 SDMIシステムにおける1つのSDMIドメインの構成を示す図である。

【図2】 SDメモリカード2の内部構成を示す図である。

【図3】 録再型PDの内部構成を示す図である。

【図4】 ライセンス管理装置1の内部構成を示す図である。

【図5】 Migrate Permission Flagを用いずにMigrateを行う場合の、第1実施形態に係るSDMIシステムの動作例を示す図である。

【図6】 Migrate Permission Flagを用いる場合の第1実施形態に係るSDMIシステムの動作例を示す図である。

【図7】 Migrate Permission Flagを用いる場合の第1実施形態に係るSDMIシステムの動作例を示す図である。

【図8】 複数のSDMIドメインのうち、1つのSDMIドメインの録再型PDがA0BをSDメモリカード2に記録した場合、このA0BについてのMigrateがどのように行われるかの動作例を示す図である。

【図9】 SDメモリカード2における物理層の構成を示す図である。

【図10】 SDメモリカード2におけるユーザデータ領域6、プロテクト領域7のディレクトリ構成、ファイル構成を示す図である。

【図11】 Title Key Entryの内部構成を示す図である。

【図12】 A0Bファイルに収録されている各A0Bが連続して再生されることにより、どのような再生内容が再生されるかを示す図である。

【図13】 TKIと、A0Bファイルと、Title Key Entryとの相互関係を示す図である。

【図14】 TKIの内部構成を示す図である。

【図15】 2つのトラックを1つに統合する場合にTKIがどのように設定されるかを示す図である。

【図16】 1つのトラックを2つのトラックに分割する場合を想定した図である。

【図17】 セキュアR/W部17、セキュアR/W部22の内部構成を示す図である。

【図18】 セキュアライト部31の内部構成を示す図である。

【図19】 セキュアリード部32の内部構成を示す図である。

【図20】 8つのAOB及び8つのTitle Key Entryについて、Migrate処理が行われる様子を示す図である。

【図21】 ローカルストレージ21のディレクトリ構成、ファイル構成を示す図である。

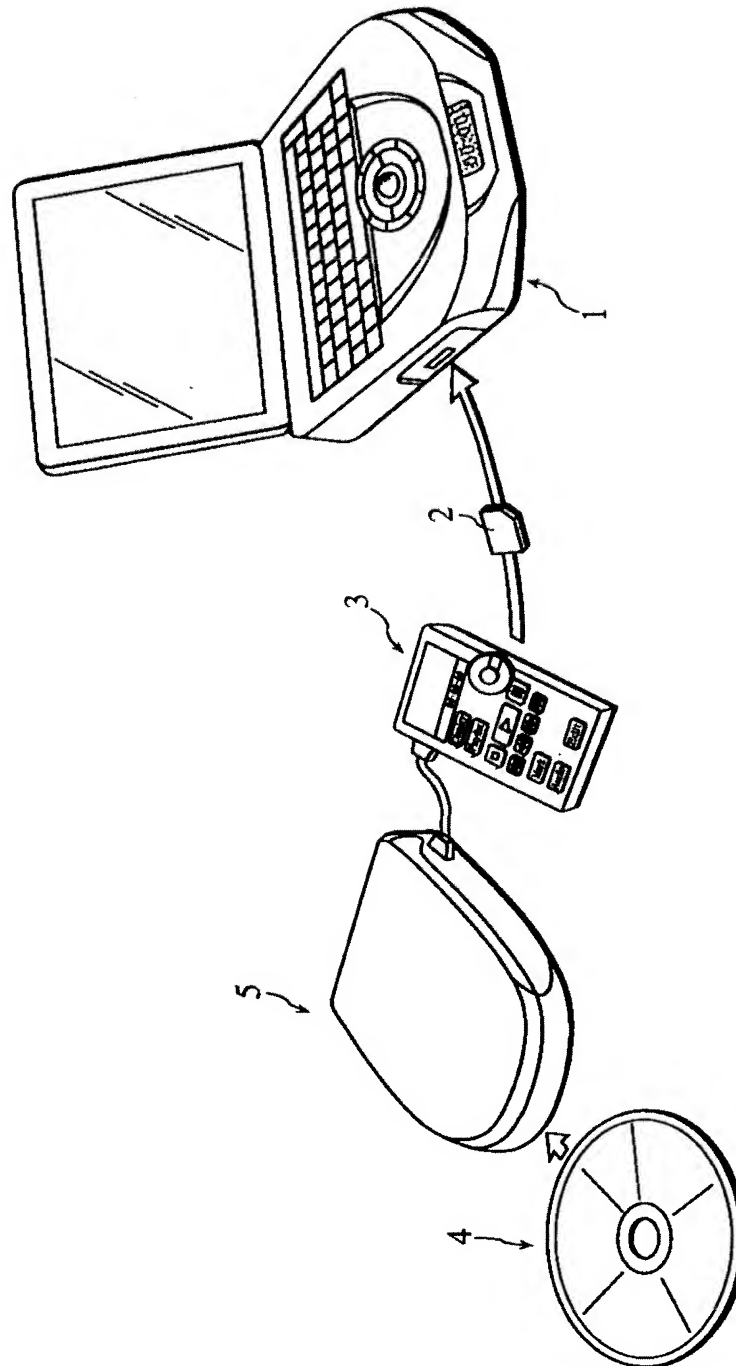
【図22】 チェックアウトにより、SDメモリカード2に8つのAOBと、8つのTitle Key Entryとが格納される様子を示す図である。

【図23】 チェックアウトが実行された後のローカルストレージ21の格納内容を示す図である。

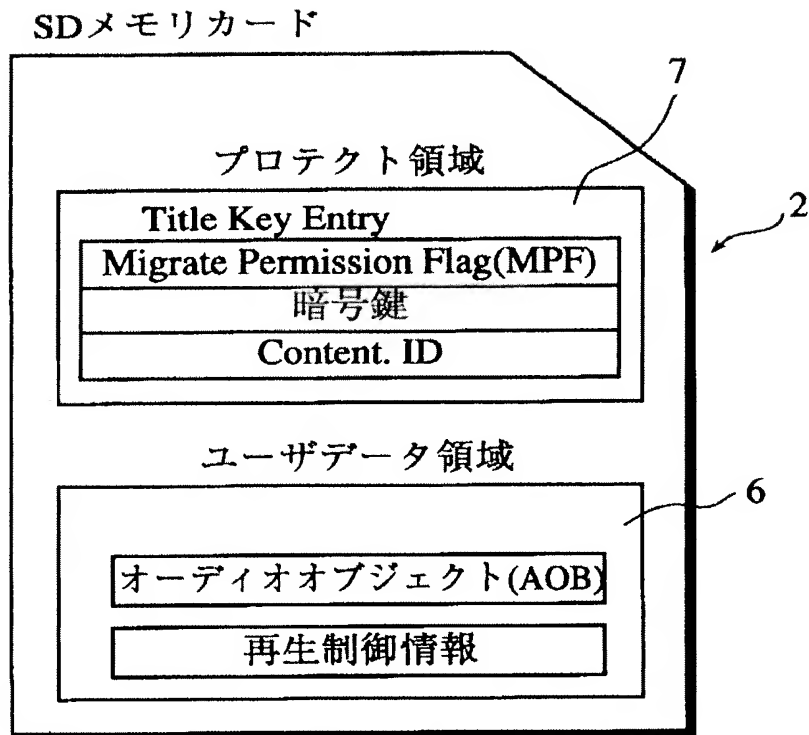
【図24】 第2実施形態に係るLCM23の処理手順を示すフローチャートである。

【図25】 第3実施形態におけるMigrate Permission Flagの設定例を示す図である。

【図1】



【図2】



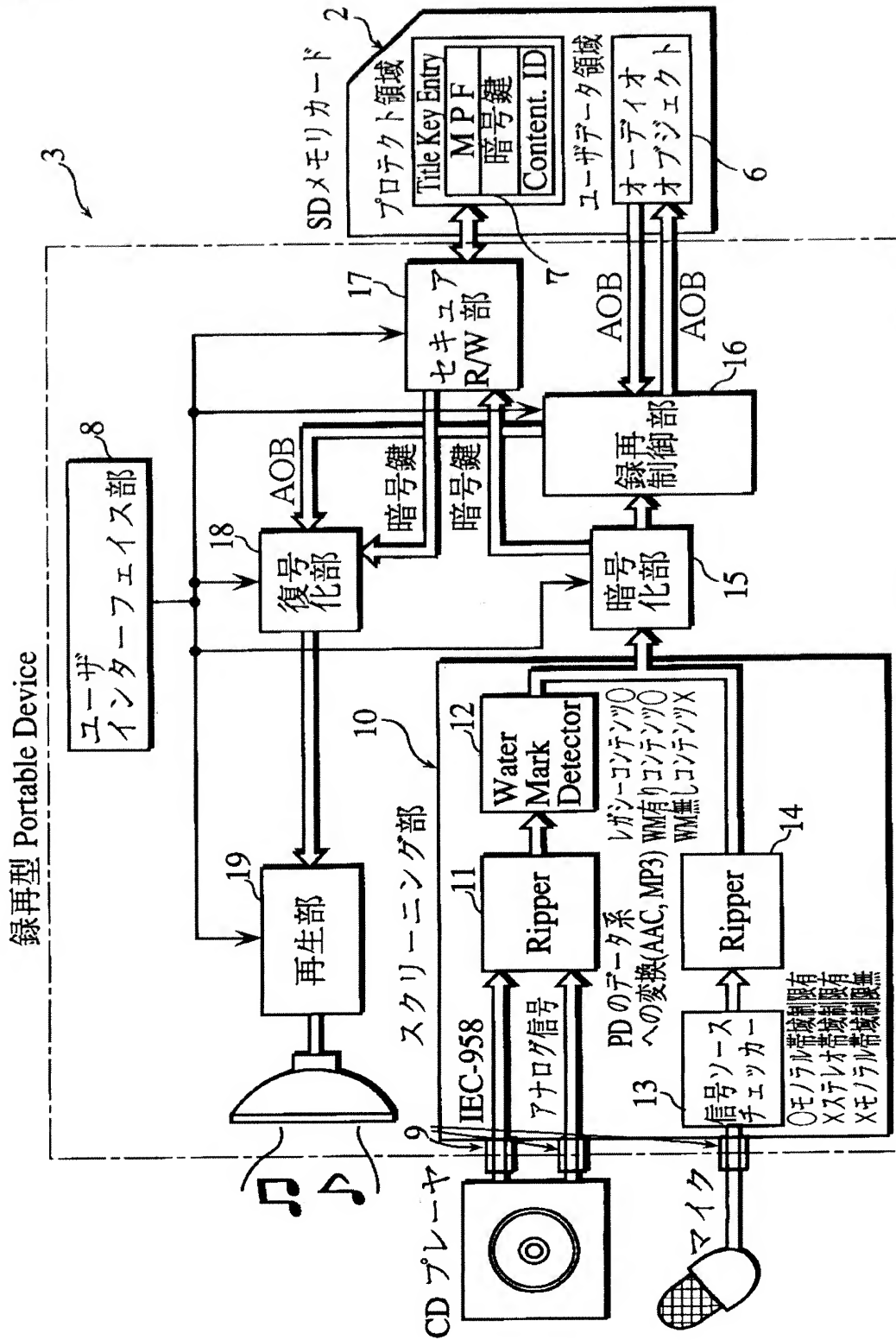
MPF : 0

Migrate が不許可  
(AOB に対応する権利管理情報が生成済み)

MPF : 1

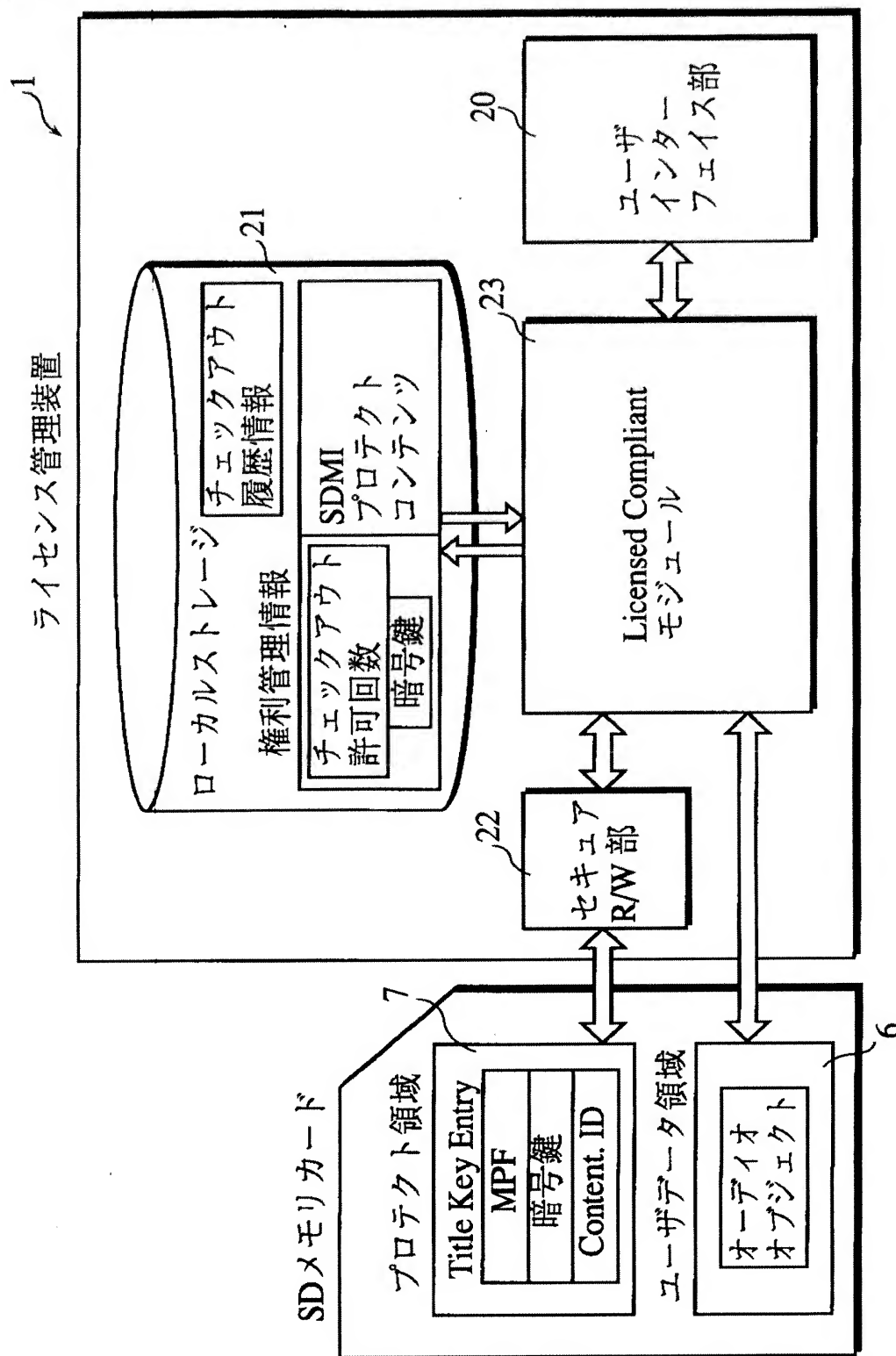
Migrate が許可  
(AOB に対応する権利管理情報が未生成)

【図3】





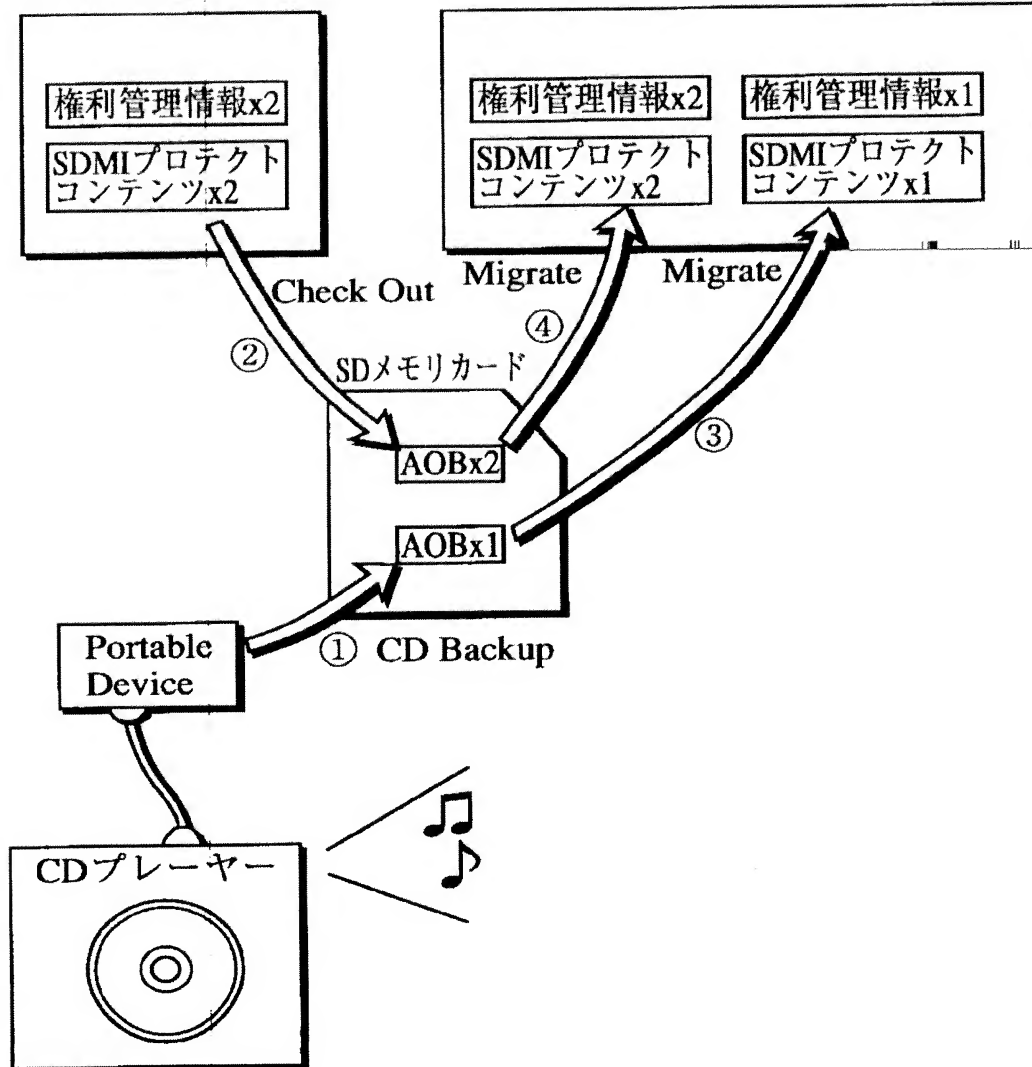
【図4】



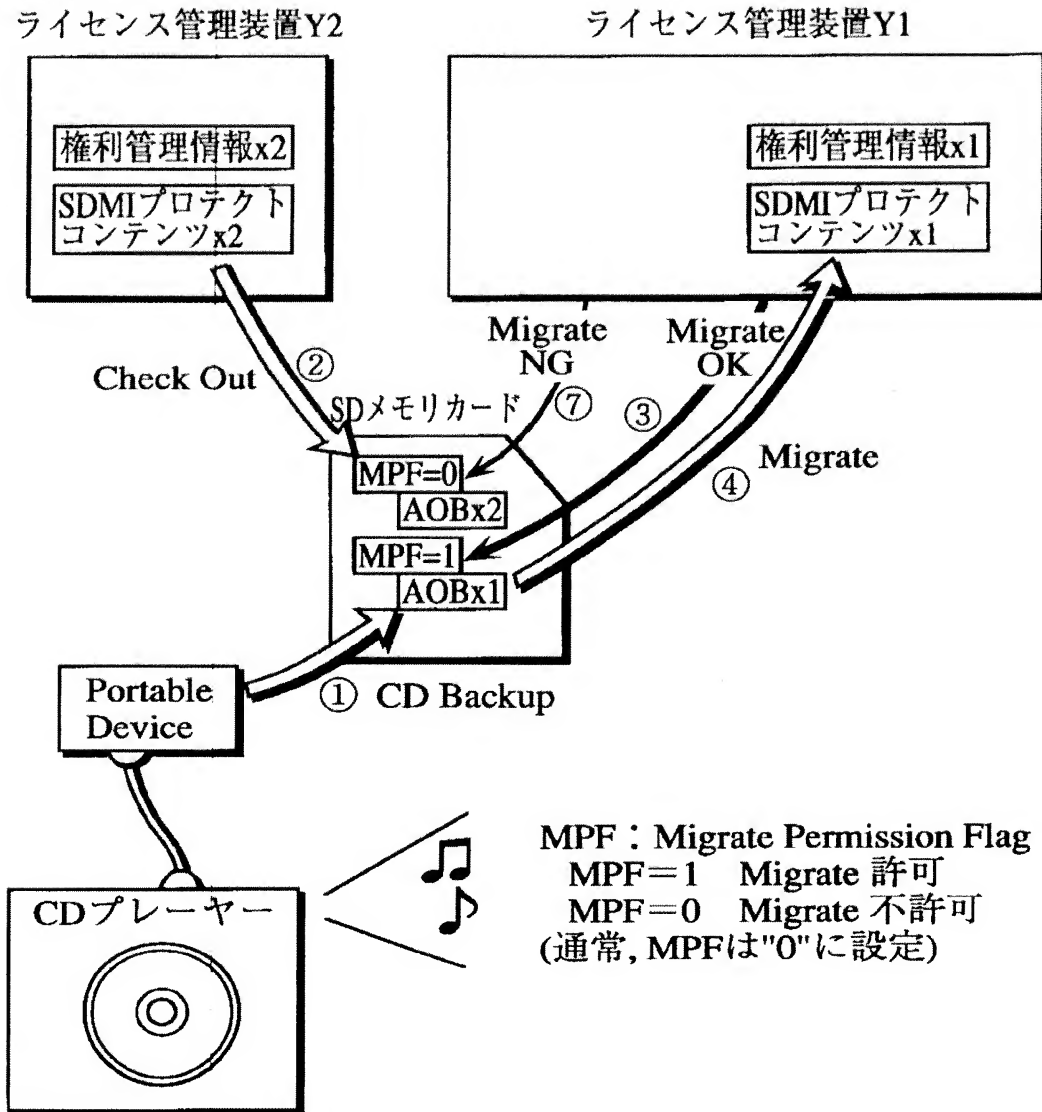
【図5】

ライセンス管理装置Y2

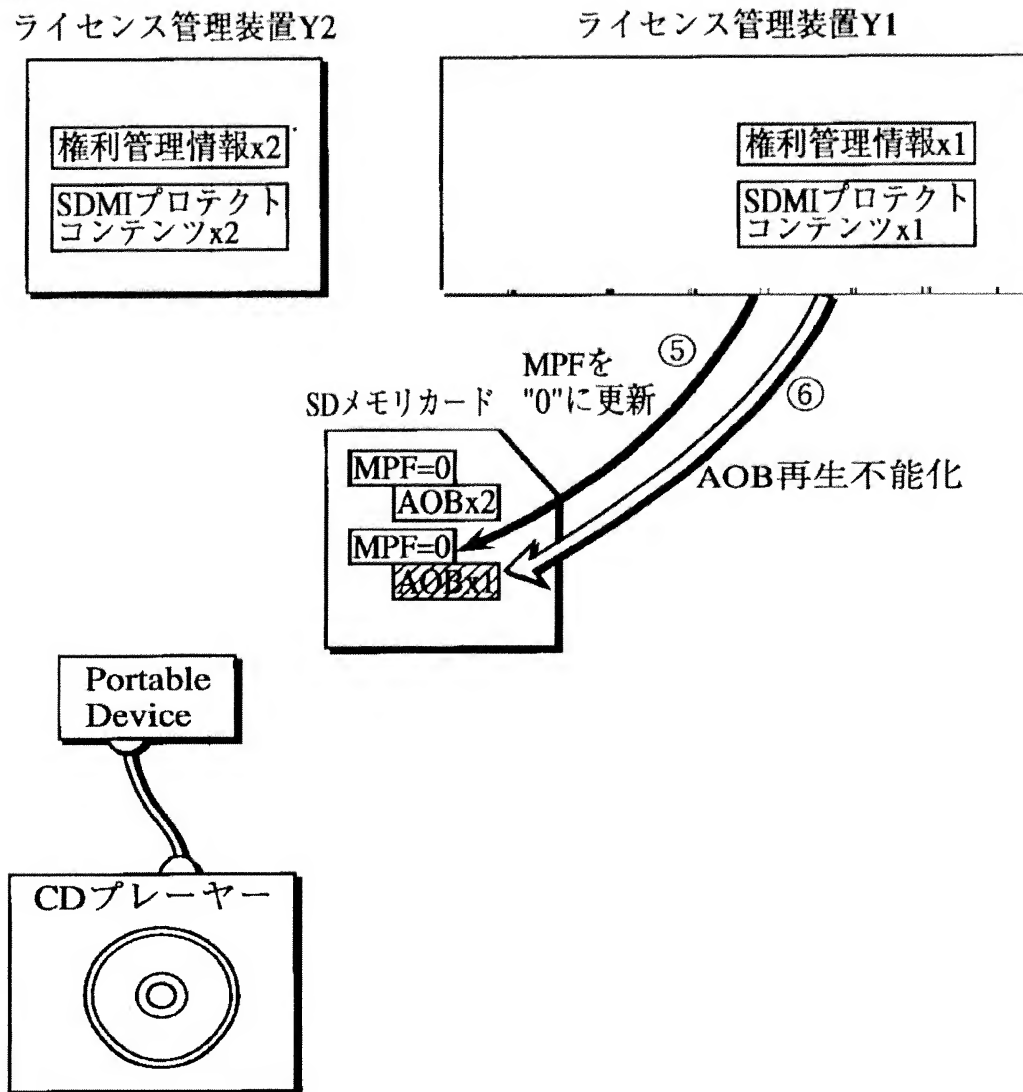
ライセンス管理装置Y1



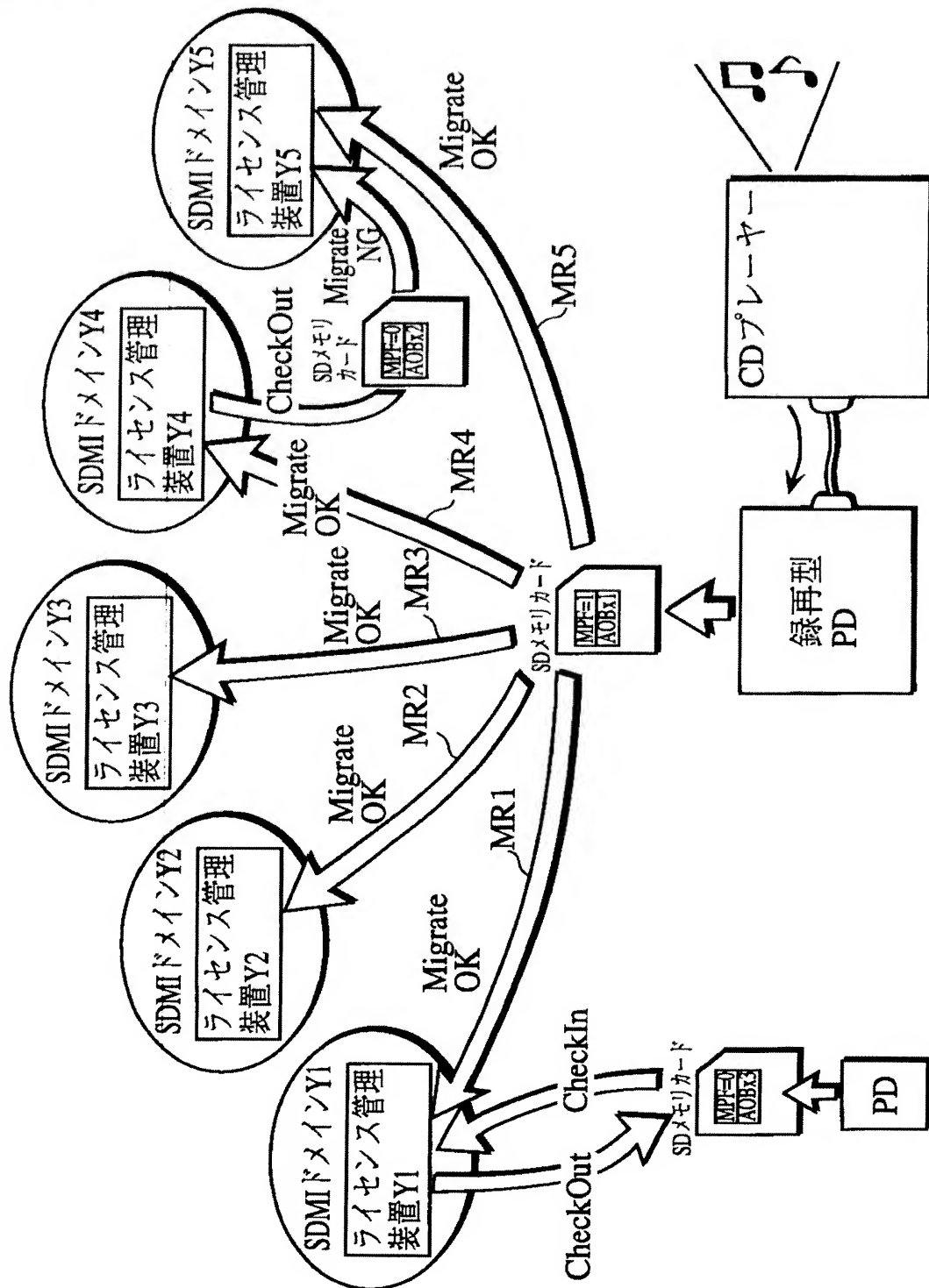
【図6】



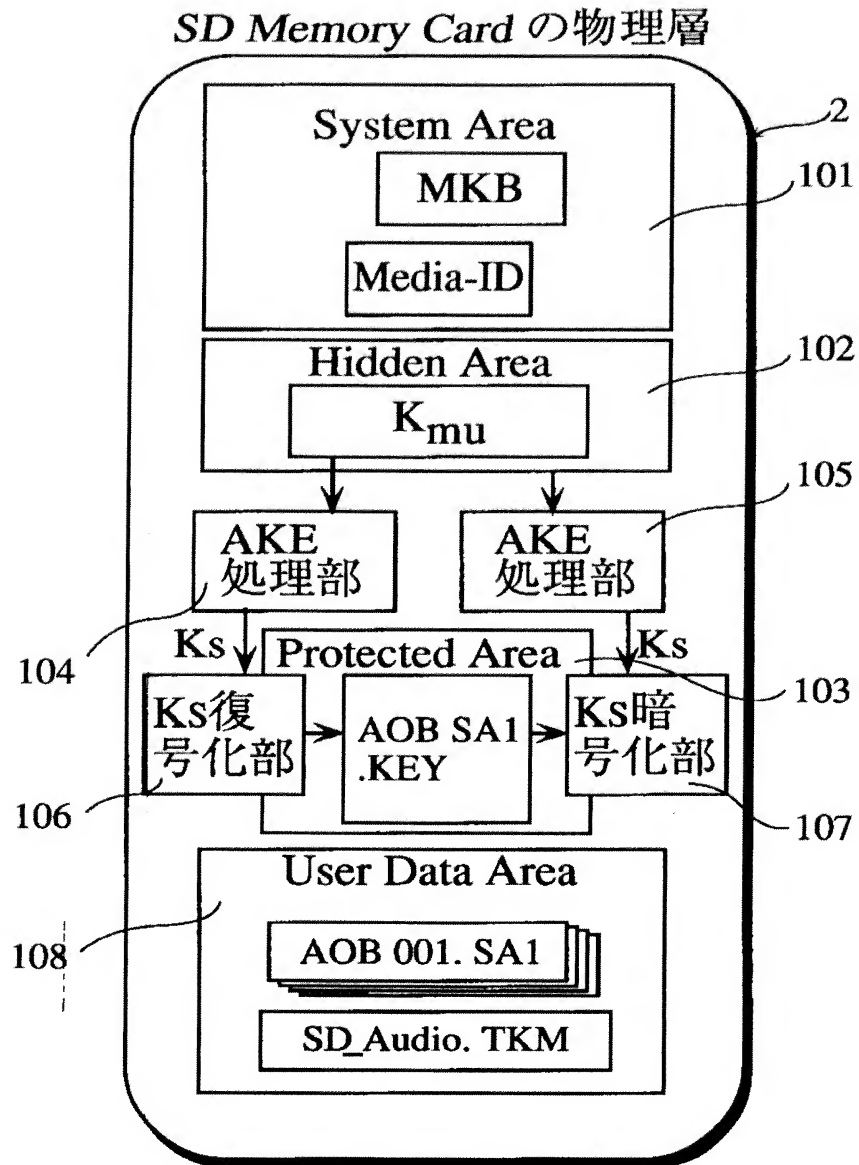
【図7】



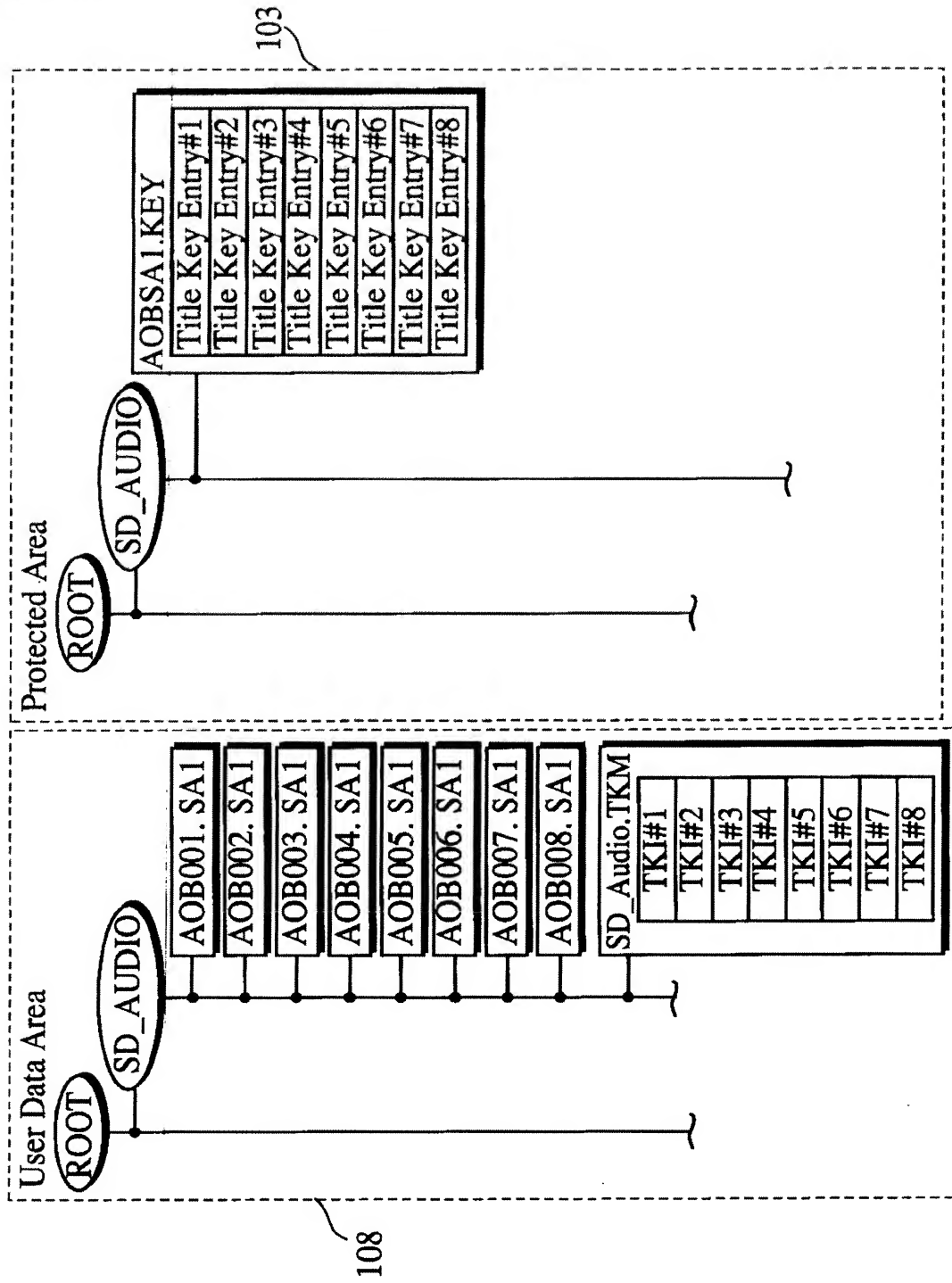
【図8】



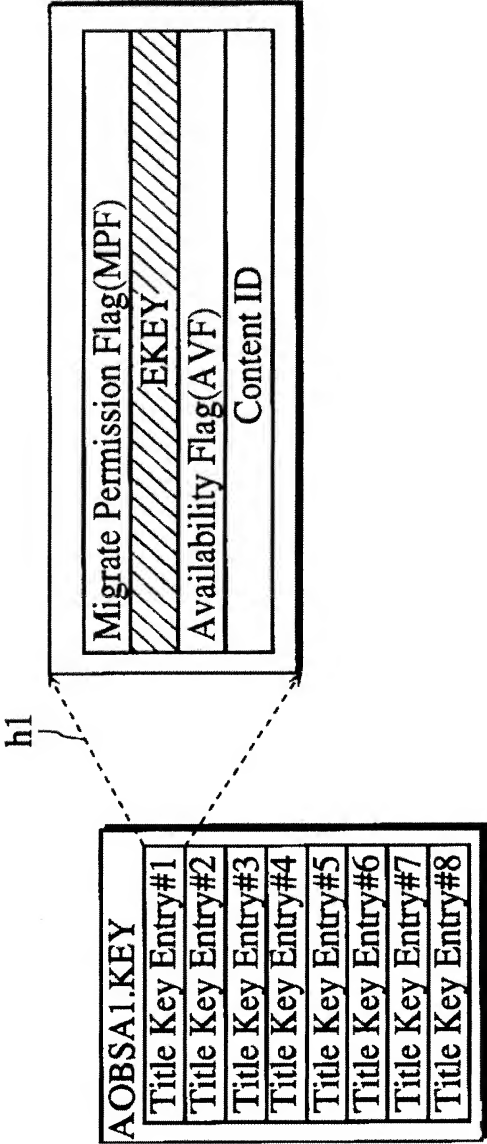
【図9】



【図10】

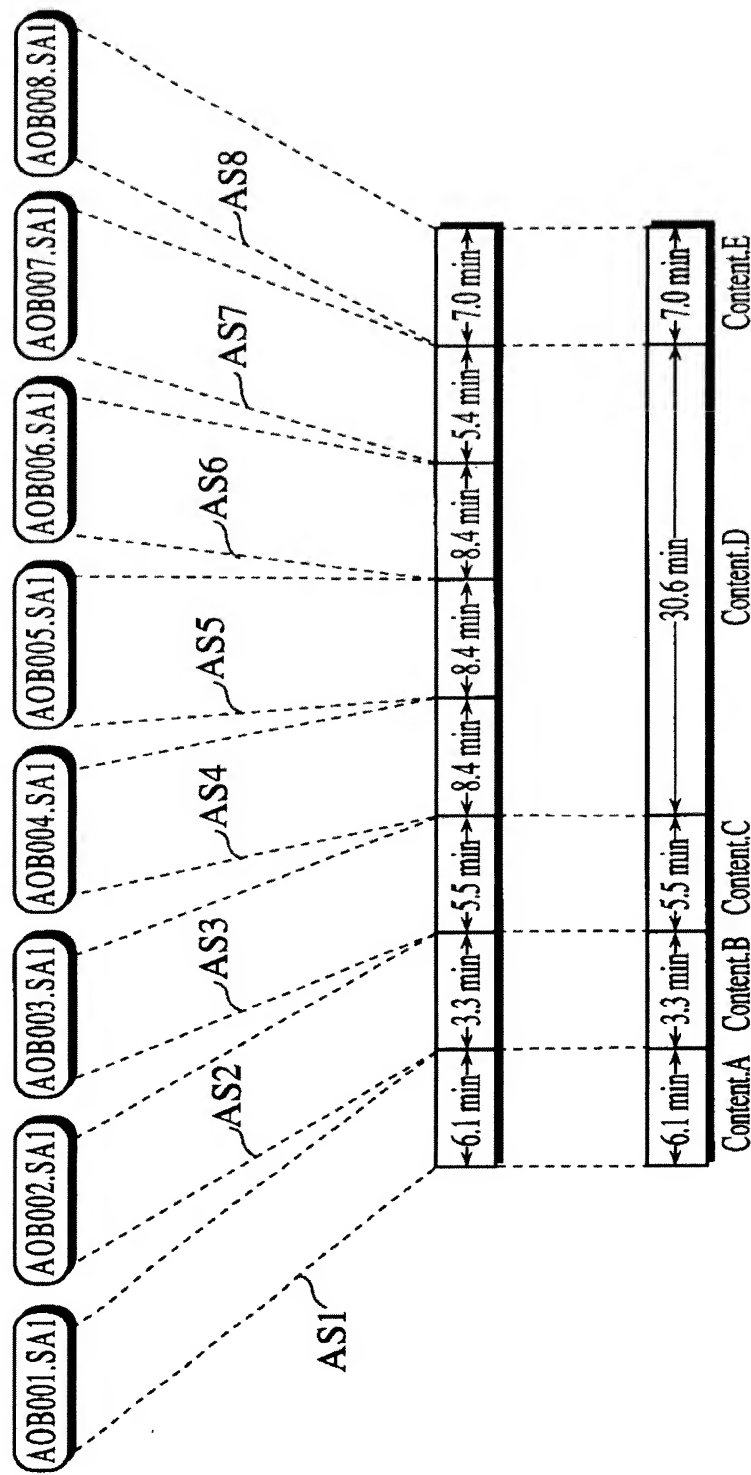


【図 1 1】

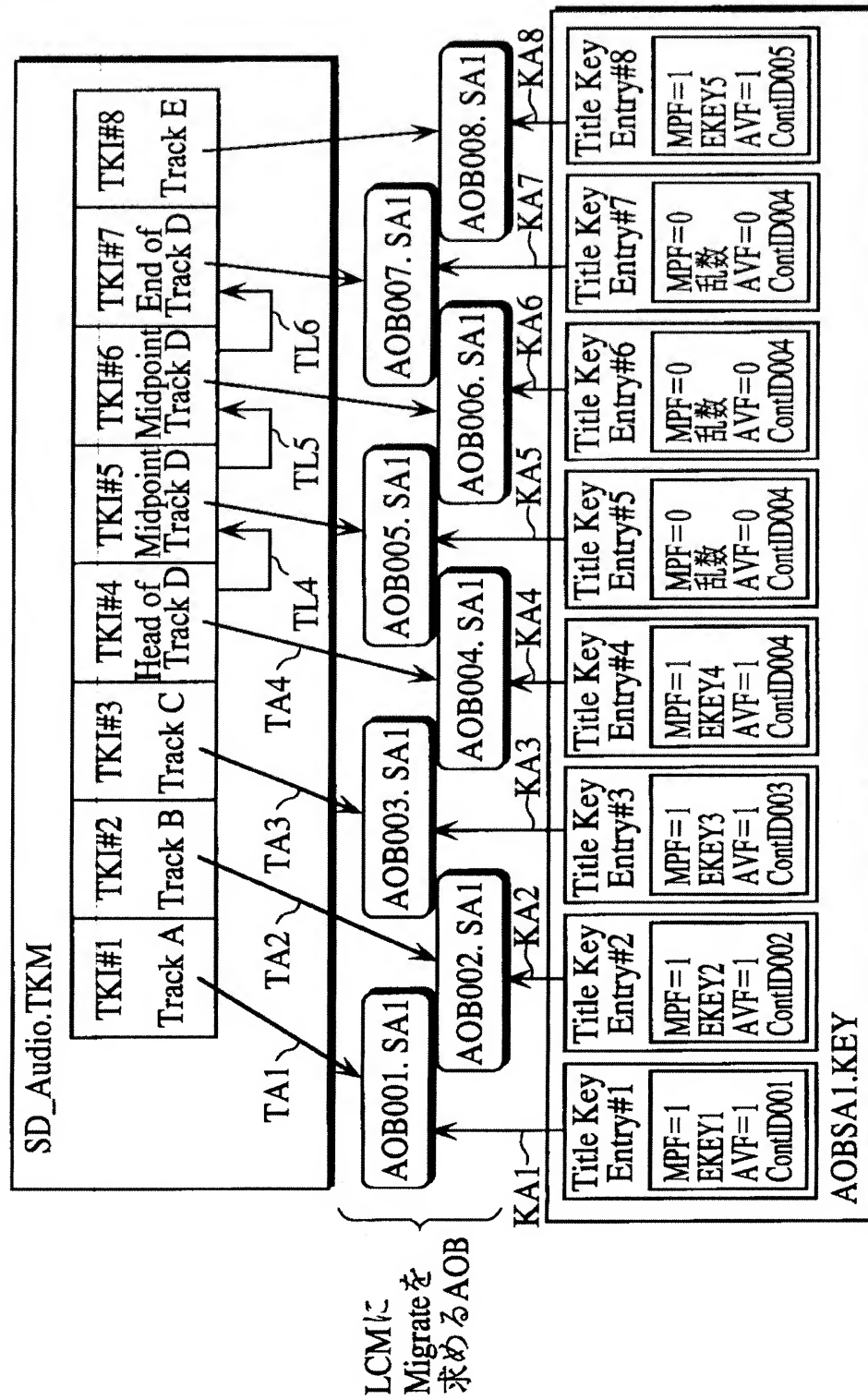




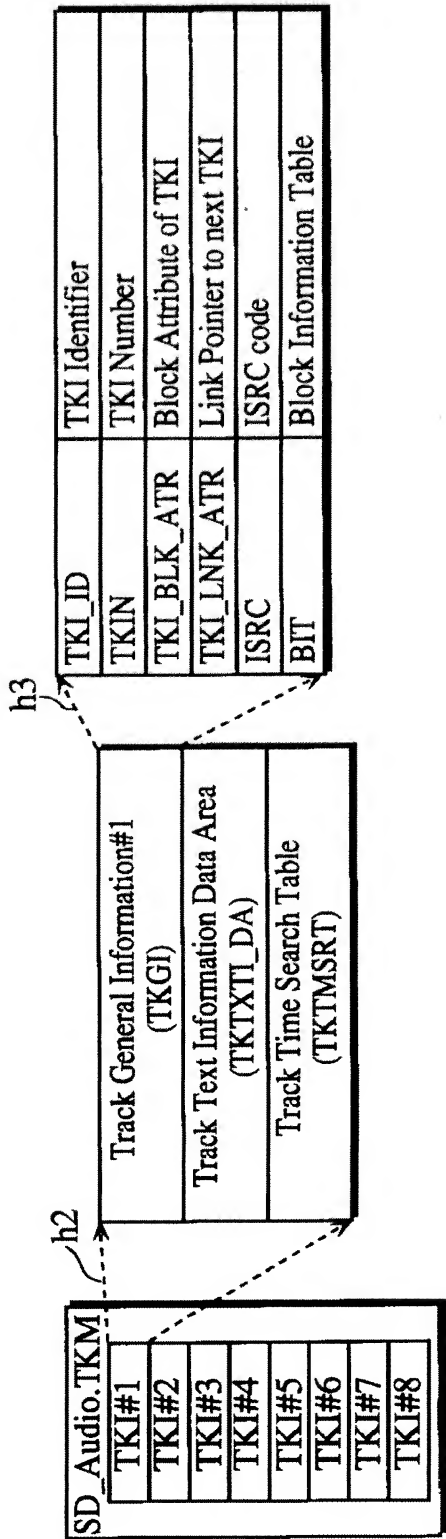
【図12】



【図13】

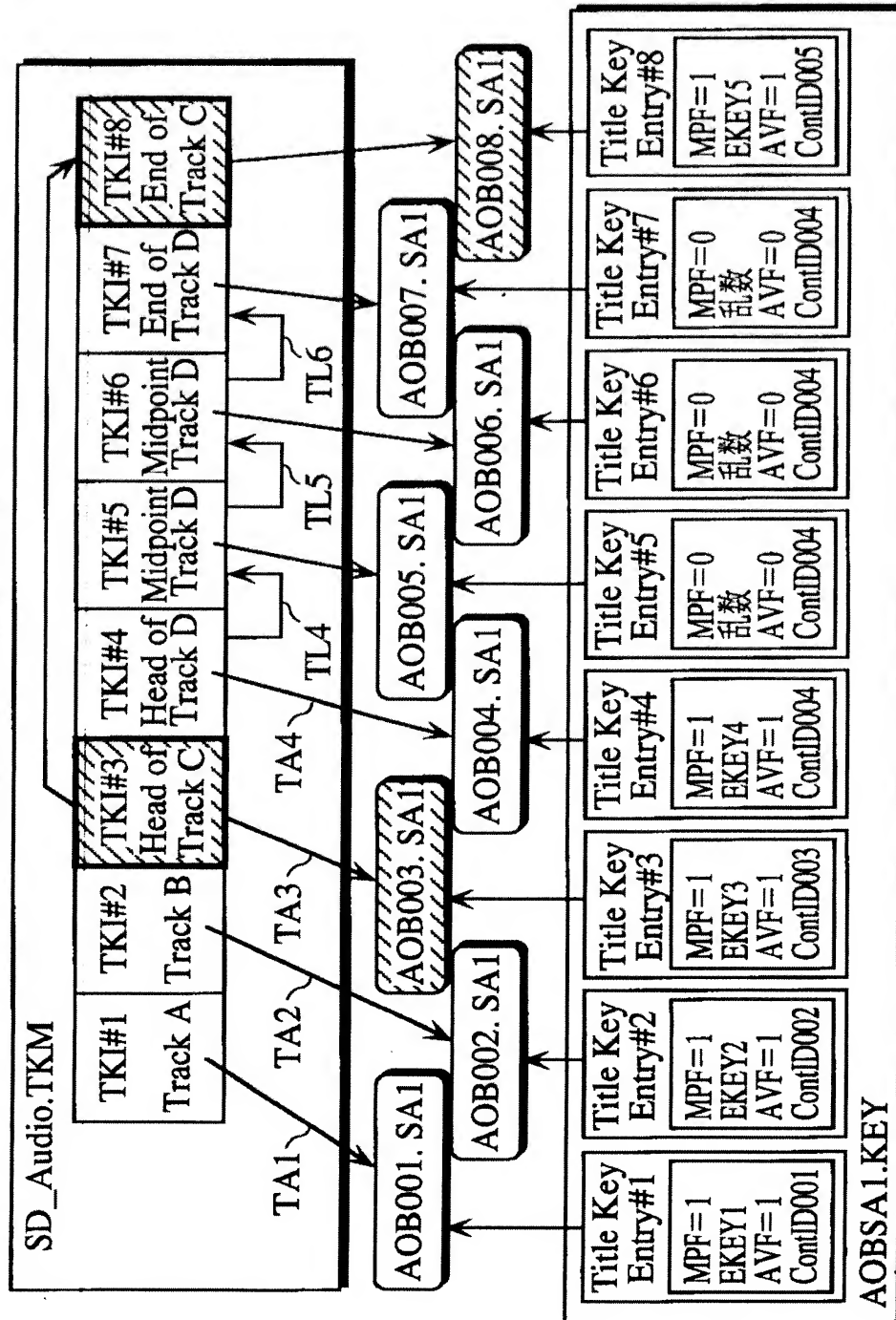


【図14】

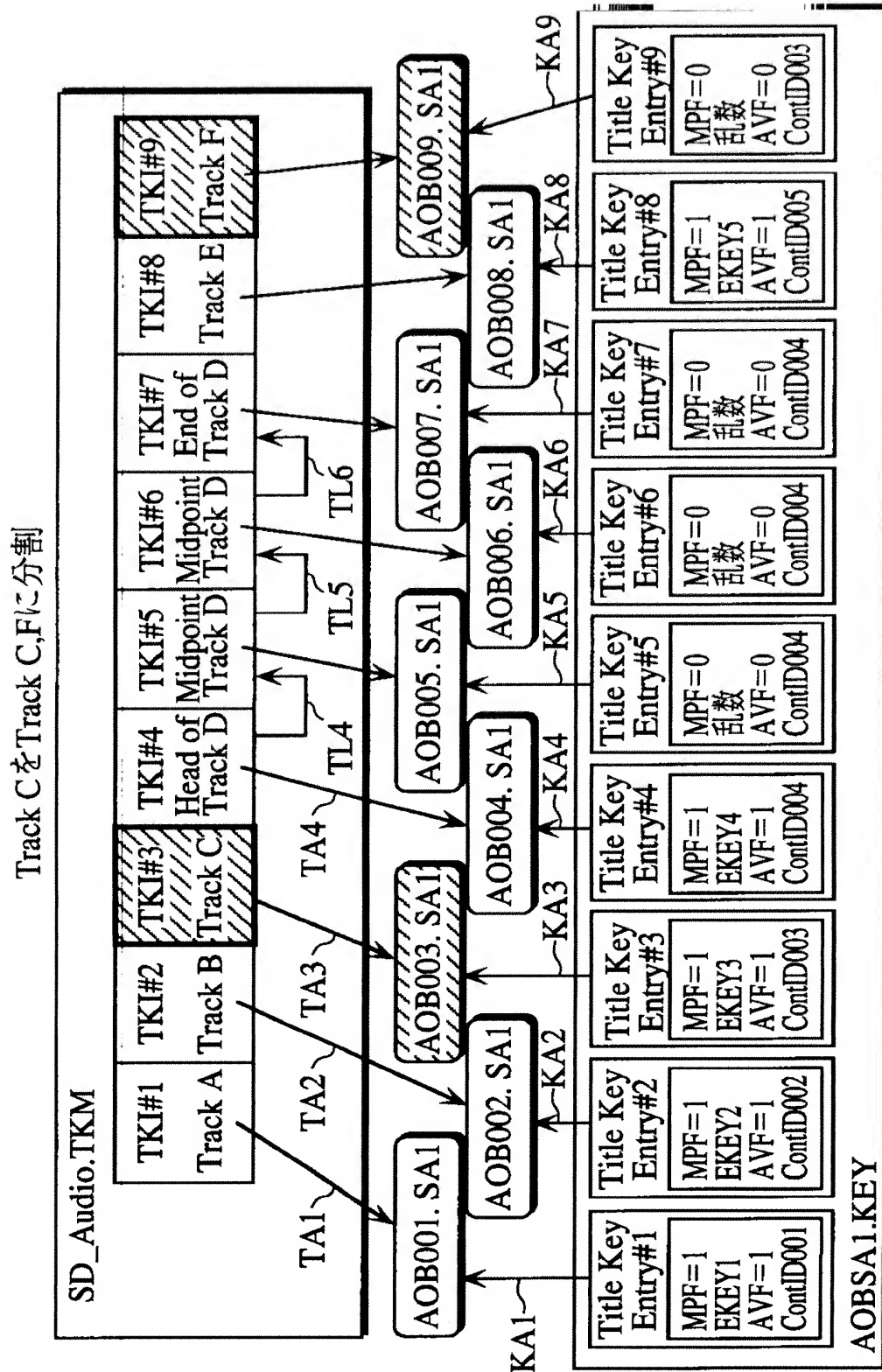


【図15】

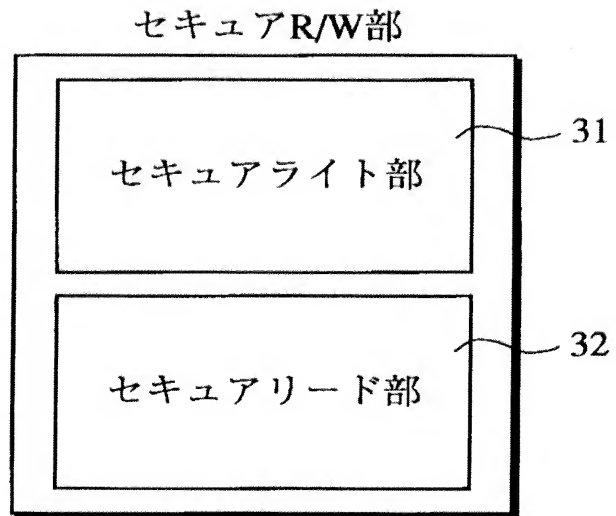
Track C, EをTrack Cに統合



【図16】

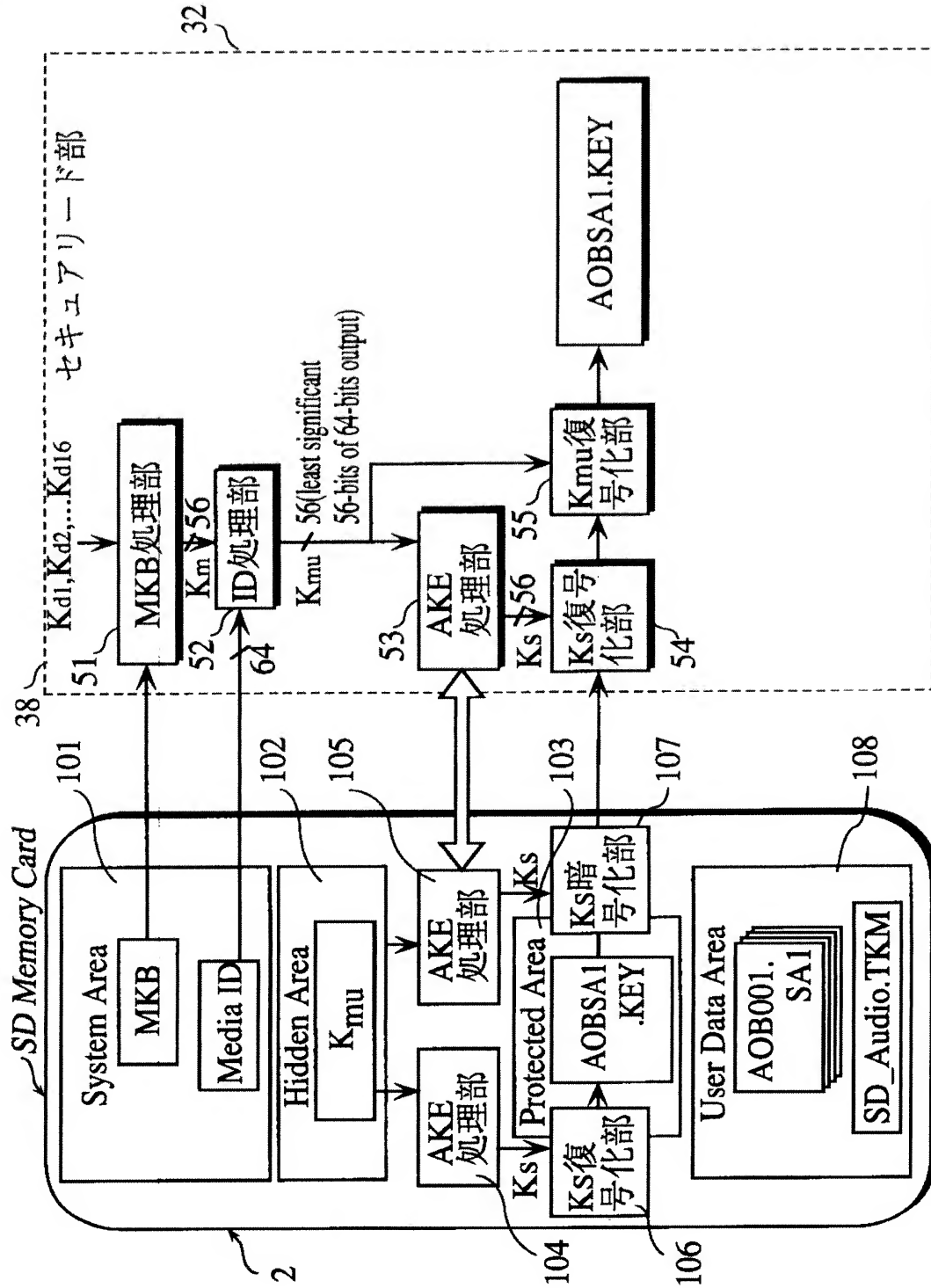


【図17】



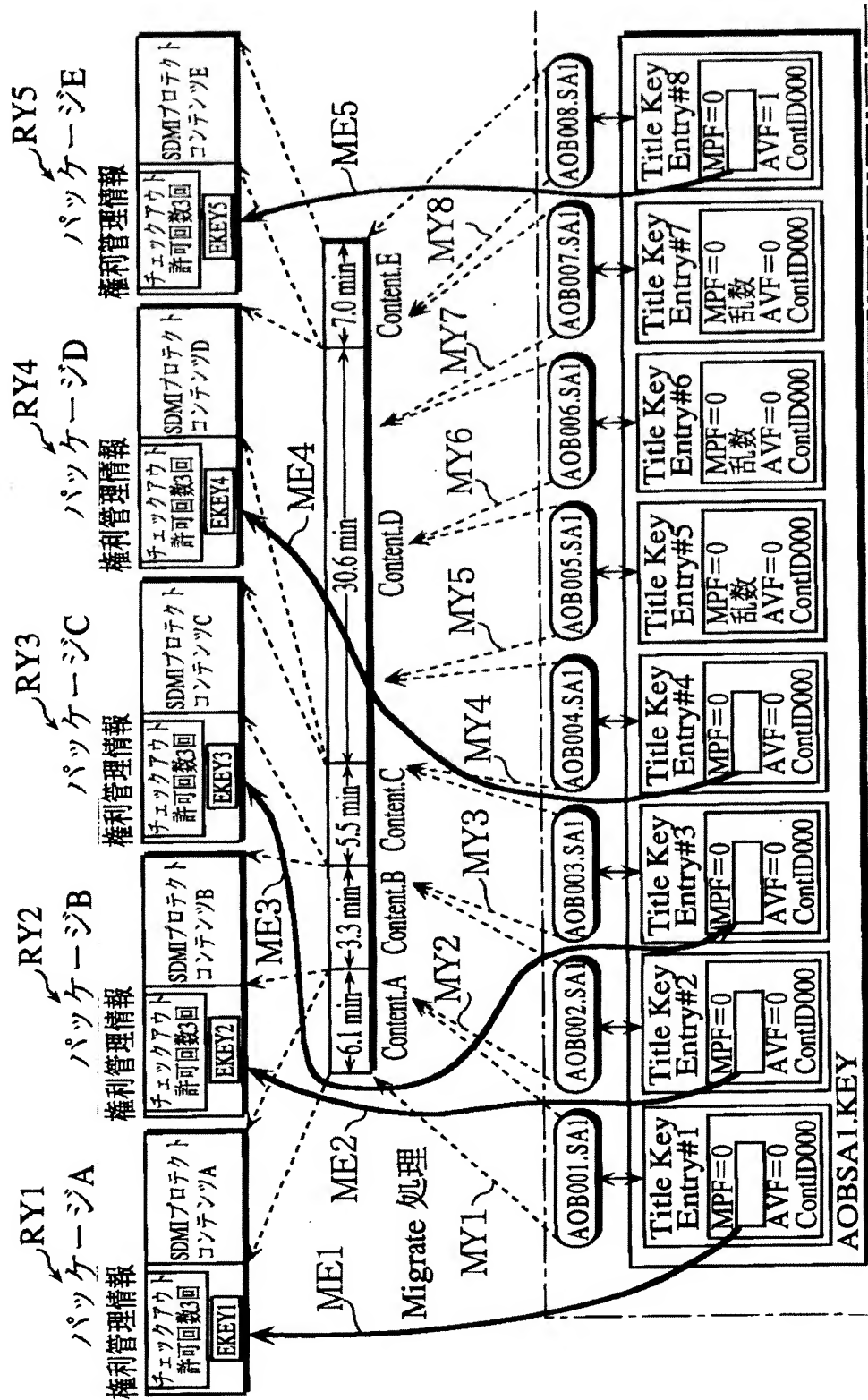


【図19】

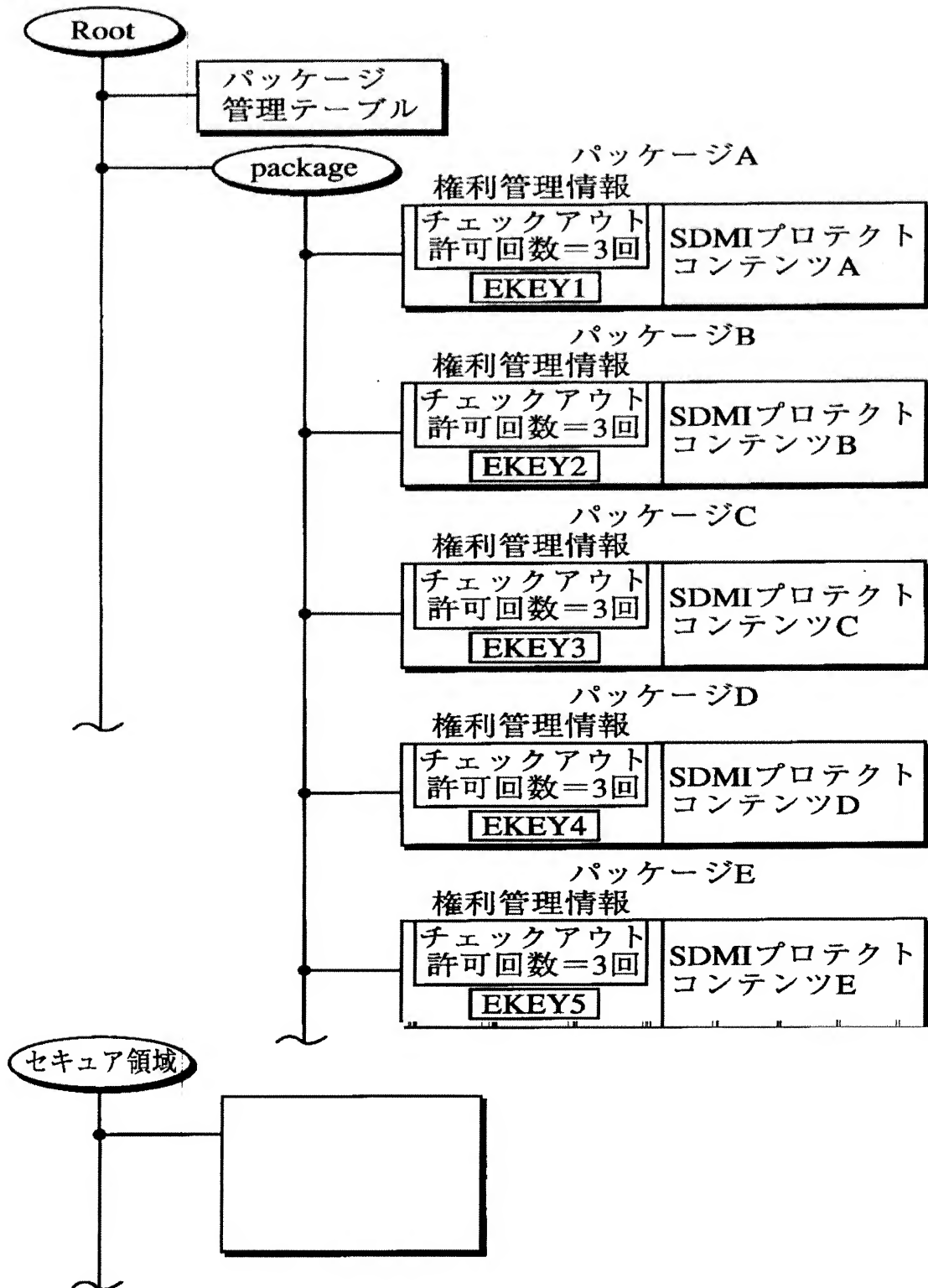




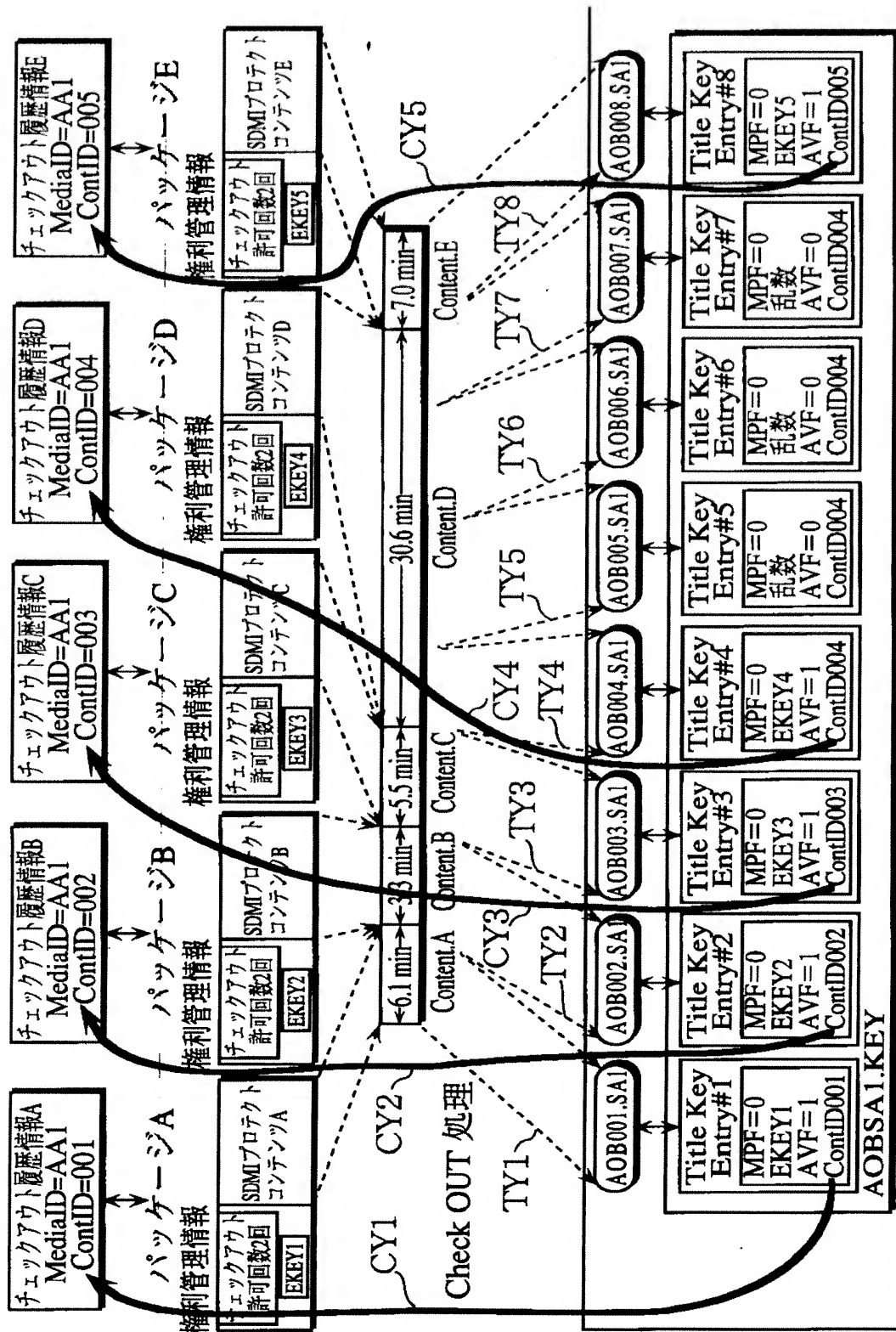
【図20】



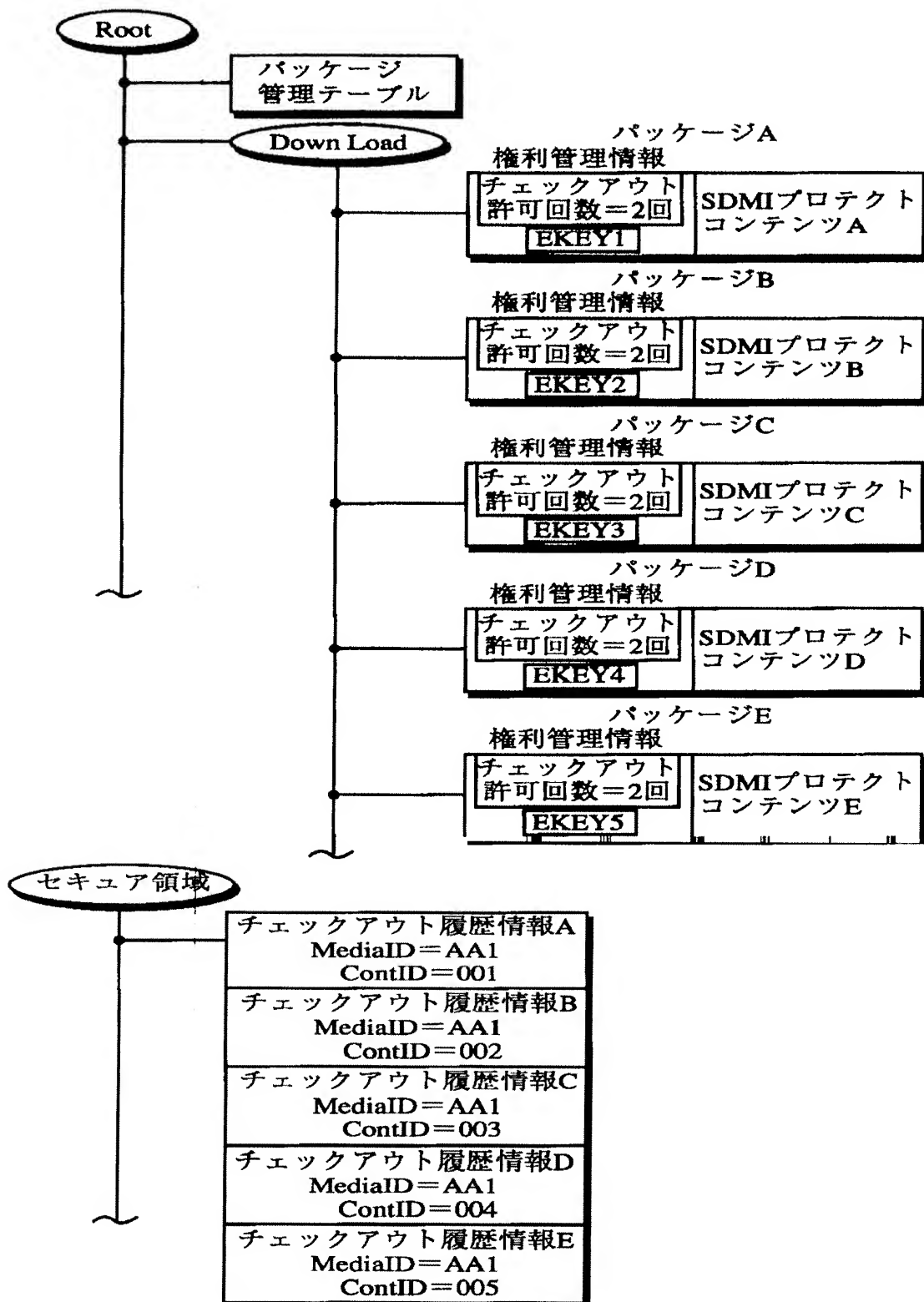
【図21】



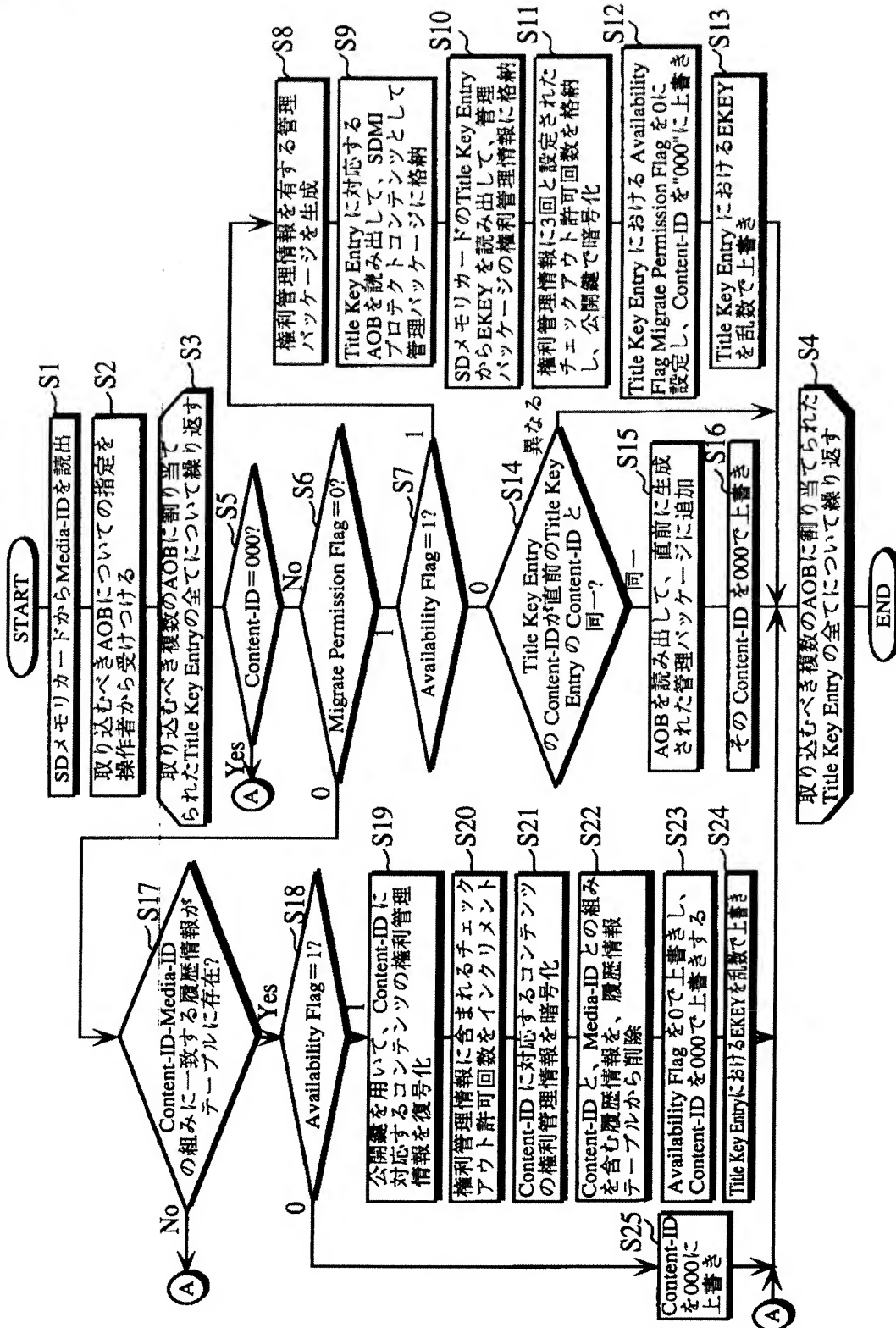
【図 22】



【図23】

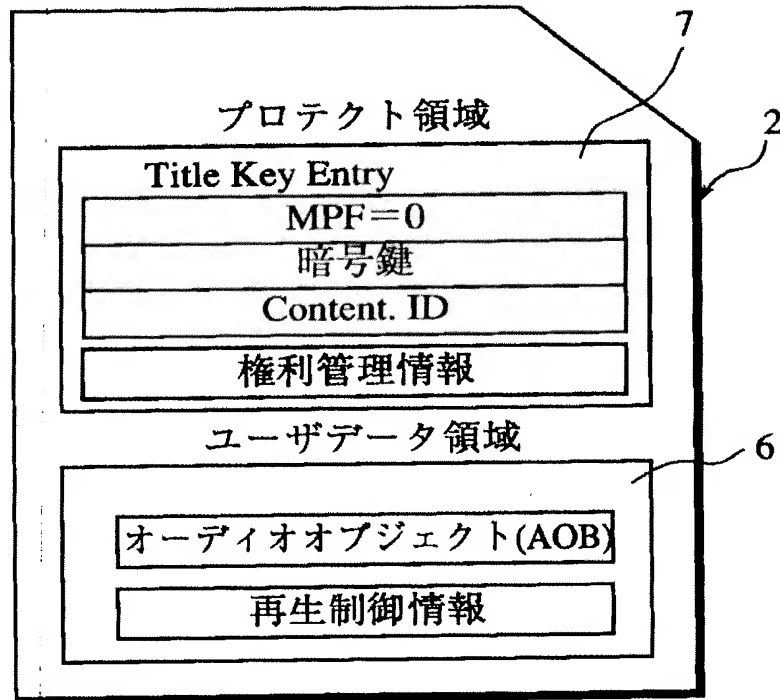


【図24】



【図25】

## SDメモ리카ード



MPF : 0

Migrate が不許可  
(AOB に対応する権利管理情報が生成済み)

MPF : 1

Migrate が許可  
(AOB に対応する権利管理情報が未生成)

## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US01/17291

| <b>A. CLASSIFICATION OF SUBJECT MATTER</b><br>IPC(7) : G06F 17/60<br>US CL : 705/59<br>According to International Patent Classification (IPC) or to both national classification and IPC  |  |   |
|---|--|---|
| <b>B. FIELDS SEARCHED</b><br>Minimum documentation searched (classification system followed by classification symbols)<br>U.S. : 705/59<br>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched<br>Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)<br>EAST  |  |   |
| <b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>   |  |   |
| Category*   | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No.   |
| A, P  | US 6,240,185 B1 (VAN WIE et al) 29 May 2001, figure 11   | 1-14  |
| A, P  | US 6,226,618 B1 (DOWNS et al) 01 May 2001, figure 5.   | 1-14  |
| A, P  | US 6,073,124 A (KRISHNAN et al) 06 June 2000, figure 11.   | 1-14  |
| A   | 5,940,504 A (GRISWOLD) 17 August 1999, figure 6.   | 1-14  |
| A   | US 5,553,143 A (ROSS et al) 03 September 1996, figure 5A.  | 1-14  |
| <input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.   |  |   |
| * Special categories of cited documents:<br>"A" document defining the general state of the art which is not considered to be of particular relevance<br>"B" earlier document published on or after the international filing date<br>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)<br>"O" document referring to an oral disclosure, use, exhibition or other means<br>"P" document published prior to the international filing date but later than the priority date claimed | "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention<br>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone<br>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art<br>"A" document member of the same patent family |   |
| Date of the actual completion of the international search<br>11 SEPTEMBER 2001  |  | Date of mailing of the international search report<br>02 NOV 2001                       |
| Name and mailing address of the ISA/US<br>Commissioner of Patents and Trademarks<br>Box PCT<br>Washington, D.C. 20231<br>Facsimile No. (703) 305-3230   |  | Authorized officer<br>THOMAS DIXON <i>Peggy Hancock</i><br>Telephone No. (703) 308-3900 |

## フロントページの続き

| (51) Int. Cl. 7 | 識別記号                           | F I     | テームコード' (参考) |   |
|-----------------|--------------------------------|---------|--------------|---|
| G 0 6 K         | 17/00                          | G 0 6 K | 17/00        | L |
|                 | 19/00                          |         | 19/00        | Q |
|                 | 19/073                         |         |              | P |
| G 1 0 L         | 19/00                          | G 1 0 L | 9/00         | N |
|                 |                                |         | 9/18         | H |
| (72) 発明者        | 小塚 雅之                          |         |              |   |
|                 | アメリカ合衆国、91006 カリフォルニア          |         |              |   |
|                 | 州アーケディア、 コイルアベニュー              |         |              |   |
|                 | 501                            |         |              |   |
| (72) 発明者        | 二階堂 正隆                         |         |              |   |
|                 | 大阪府四條畷市田原台 5 丁目10ー20           |         |              |   |
| F ターム (参考)      | 5B017 AA03 AA06 BA07 BA09 CA09 |         |              |   |
|                 | CA16                           |         |              |   |
|                 | 5B035 AA13 BB09 BC00 CA11 CA29 |         |              |   |
|                 | CA38                           |         |              |   |
|                 | 5B058 CA23 KA01 KA02 KA04 KA31 |         |              |   |
|                 | KA35 YA20                      |         |              |   |